



MAX Series

User Manual

Peplink Products:

BR2

Peplink Firmware 8.3.0
September 2023

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice.

Copyright © 2021 Peplink Pepwave Ltd. All Rights Reserved. Pepwave and the Pepwave logo are trademarks of Peplink International Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

Table of Contents

Introduction and Scope	6
Glossary	8
1 Product Features	9
1.1 Supported Network Features	9
1.2 Other Supported Features	12
2 BR2 Overview	13
2.1 Panel Appearance	13
3 Advanced Feature Summary	14
3.1 Drop-in Mode and LAN Bypass: Transparent Deployment	14
3.2 QoS: Clearer VoIP	14
3.3 Per-User Bandwidth Control	15
3.4 High Availability via VRRP	15
3.5 USB Modem and Android Tethering	16
3.6 Built-In Remote User VPN Support	16
3.7 SIM-card USSD support	17
3.8 KVM Virtualization	17
3.9 DPI Engine	18
3.10 NetFlow	18
3.11 Wi-Fi Air Monitoring	18
3.12 SP Default Configuration	18
3.13 Peplink Relay	19
3.14 DNS over HTTPS (DoH)	19
3.15 Peplink InTouch	19
3.16 Synergy Mode	19
3.17 Virtual WAN on VLAN	20
4 Installation	21
4.1 Preparation	21
4.2 Constructing the Network	21
4.3 Configuring the Network Environment	22
5 Connecting to the Web Admin Interface	23
6 SpeedFusion Connect Protect	25
6.1 Activate SpeedFusion Connect Protect	25
6.2 Enable SpeedFusion Connect Protect	26
6.3 Route by Cloud Application	31

6.4 Route by Wi-Fi SSID	32
6.5 Route by LAN Client	33
7 Configuring the LAN Interface(s)	35
7.1 Basic Settings	35
7.2 Port Settings	44
7.3 Captive Portal	45
8 Configuring the WAN Interface(s)	49
8.1 Ethernet WAN	52
8.2 Cellular WAN	60
8.3 Wi-Fi WAN	66
8.4 WAN Connection Settings (Common)	70
8.5 WAN Health Check	71
8.6 Bandwidth Allowance Monitoring	74
8.7 Additional Public IP address	75
8.8 Dynamic DNS Settings	75
9 SpeedFusion VPN	77
9.1 SpeedFusion VPN	78
10 IPsec VPN	88
10.1 IPsec VPN Settings	88
10.2 GRE Tunnel	92
11 OpenVPN	94
12 Outbound Policy	95
12.1 Adding Rules for Outbound Policy	95
13 Port Forwarding	105
13.1 UPnP / NAT-PMP Settings	107
14 NAT Mappings	108
15 Media Fast	110
15.1 Setting Up MediaFast Content Caching	110
15.2 Viewing MediaFast Statistics	112
15.3 Prefetch Schedule	113
16 Edge Computing	115
16.1 Configuring the ContentHub	115
16.2 Configure a website for ContentHub	115
16.3 Configure an application for ContentHub	117
17 Docker	120
18 KVM	121
19 QoS	122

19.1 User Groups	122
19.2 Bandwidth Control	123
19.3 Application Queue	123
19.4 Application	124
20 Firewall	126
20.1 Access Rules	127
20.2 Content Blocking	135
21 Routing Protocols	137
21.1 OSPF & RIPv2	137
21.2 BGP	139
22 Remote User Access	144
23 Miscellaneous Settings	147
23.1 High Availability	147
23.2 RADIUS Server	151
23.3 Certificate Manager	153
23.4 Service Forwarding	154
23.5 Service Passthrough	157
23.6 UART	158
23.7 GPS Forwarding	160
23.8 Ignition Sensing	161
Ignition Sensing installation	161
GPIO Menu	163
23.9 NTP Server	164
23.10 Grouped Networks	165
23.11 Remote SIM Management	166
23.12 SIM Toolkit	168
23.13 UDP Relay	170
24 AP	171
24.1 AP Controller	171
24.2 Wireless SSID	171
24.3 Wireless Mesh	177
24.4 Settings	178
25 AP Controller Status	185
25.1 Info	185
25.2 Access Point	187
25.3 Wireless SSID	190
25.4 Wireless Client	191

25.5 Mesh / WDS	192
25.6 Nearby Device	193
25.7 Event Log	193
26 Toolbox	194
27 System	195
27.1 Admin Security	195
27.2 Firmware	200
27.3 Time	202
27.4 Schedule	203
27.5 Email Notification	204
27.6 Event Log	207
27.7 SNMP	208
27.8 SMS Control	210
27.9 InControl	211
27.10 Configuration	212
27.11 Feature Add-ons	213
27.12 Reboot	213
28 Tools	214
28.1 Ping	214
28.2 Traceroute Test	215
28.3 Wake-on-LAN	215
28.4 WAN Analysis	216
28.5 CLI (Command Line Interface Support)	219
29 Status	220
29.1 Device	220
29.2 GPS Data	222
29.3 Active Sessions	223
29.4 Client List	225
29.5 UPnP / NAT-PMP	226
29.6 OSPF & RIPv2	227
29.7 BGP	227
29.8 SpeedFusion VPN	227
29.9 Event Log	232
30 WAN Quality	234
31 Usage Reports	235
31.1 Real-Time	235
31.2 Hourly	236

31.3 Daily	237
31.4 Monthly	238
Appendix A: Restoration of Factory Defaults	240
Appendix B: Overview of ports used by Peplink SD-WAN routers and other Peplink services	241

Introduction and Scope

Pepwave routers provide link aggregation and load balancing across multiple WAN connections, allowing a combination of technologies like 3G HSDPA, EVDO, 4G LTE, Wi-Fi, external WiMAX dongle, and satellite to be utilized to connect to the Internet.

The MAX wireless SD-WAN router series has a wide range of products suitable for many different deployments and markets. Entry level SD-WAN models such as the MAX BR1 are suitable for SMEs or branch offices. High-capacity SD-WAN routers such as the MAX HD2 are suitable for larger organizations and head offices.

This manual covers setting up Pepwave routers and provides an introduction to their features and usage.

Tips

Want to know more about Pepwave routers? Visit our YouTube Channel for a video introduction!



<https://youtu.be/13M-JHRAICA>

Glossary

The following terms, acronyms, and abbreviations are frequently used in this manual:

Term	Definition
3G	3rd generation standards for wireless communications (e.g., HSDPA)
4G	4th generation standards for wireless communications (e.g., LTE)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EVDO	Evolution-Data Optimized
FQDN	Fully Qualified Domain Name
HSDPA	High-Speed Downlink Packet Access
HTTP	Hyper-Text Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
MAC Address	Media Access Control Address
MTU	Maximum Transmission Unit
MSS	Maximum Segment Size
NAT	Network Address Translation
PPPoE	Point to Point Protocol over Ethernet
QoS	Quality of Service
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network

1 Product Features

Pepwave routers enable all LAN users to share broadband Internet connections, and they provide advanced features to enhance Internet access. Our Max BR wireless routers support multiple SIM cards. They can be configured to switch from using one SIM card to another SIM card according to different criteria, including wireless network reliability and data usage.

Our MAX HD series wireless routers are embedded with multiple 4G LTE modems, and allow simultaneous wireless Internet connections through multiple wireless networks. The wireless Internet connections can be bonded together using our SpeedFusion technology. This allows better reliability, larger bandwidth, and increased wireless coverage compared to use only one 4G LTE modem.

Below is a list of supported features on Pepwave routers. Features vary by model. For more information, please see peplink.com/products.

1.1 Supported Network Features

1.1.1 WAN

- Ethernet WAN connection in full/half duplex
- Static IP support for PPPoE
- Built-in cellular modems
- USB mobile connection(s)
- Wi-Fi WAN connection
- Network address translation (NAT)/port address translation (PAT)
- Inbound and outbound NAT mapping
- IPsec NAT-T and PPTP packet passthrough
- MAC address clone and passthrough
- Customizable MTU and MSS values
- WAN connection health check
- Dynamic DNS (supported service providers: changeip.com, dyndns.org, no-ip.org, tzo.com and DNS-O-Matic)
- Ping, DNS lookup, and HTTP-based health check

1.1.2 LAN

- Wi-Fi AP
- Ethernet LAN ports
- DHCP server on LAN

- Extended DHCP option support
- Static routing rules
- VLAN on LAN support

1.1.3 VPN

- SpeedFusion VPN with SpeedFusion™
- SpeedFusion VPN performance analyzer
- X.509 certificate support
- VPN load balancing and failover among selected WAN connections
- Bandwidth bonding and failover among selected WAN connections
- IPsec VPN for network-to-network connections (works with Cisco and Juniper)
- Ability to route Internet traffic to a remote VPN peer
- Optional pre-shared key setting
- SpeedFusion™ throughput, ping, and traceroute tests
- PPTP server
- PPTP and IPsec passthrough

1.1.4 Firewall

- Outbound (LAN to WAN) firewall rules
- Inbound (WAN to LAN) firewall rules per WAN connection
- Intrusion detection and prevention
- Specification of NAT mappings
- Outbound firewall rules can be defined by destination domain name

1.1.5 Captive Portal

- Splash screen of open networks, login page for secure networks
- Customizable built-in captive portal
- Supports linking to outside page for captive portal

1.1.6 Outbound Policy

- Link load distribution per TCP/UDP service
- Persistent routing for specified source and/or destination IP addresses per TCP/UDP service
- Traffic prioritization and DSL optimization
- Prioritize and route traffic to VPN tunnels with Priority and Enforced algorithms

1.1.7 AP Controller

- Configure and manage Pepwave AP devices
- Review the status of connected APs

1.1.8 QoS

- Quality of service for different applications and custom protocols
- User group classification for different service levels
- Bandwidth usage control and monitoring on group- and user-level
- Application prioritization for custom protocols and DSL/cable optimization

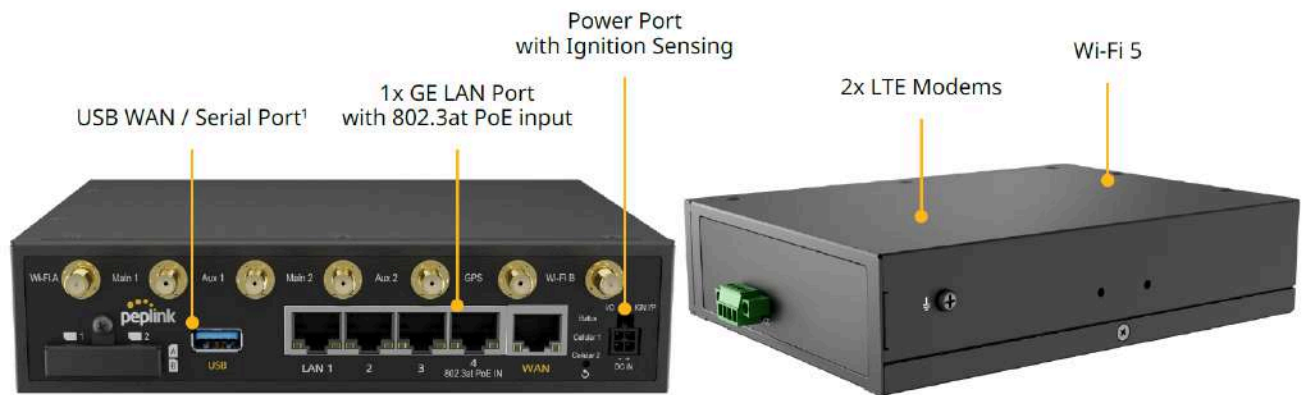
1.2 Other Supported Features

- User-friendly web-based administration interface
- HTTP and HTTPS support for web admin interface (default redirection to HTTPS)
- Configurable web administration port and administrator password
- Firmware upgrades, configuration backups, ping, and traceroute via web admin interface
- Remote web-based configuration (via WAN and LAN interfaces)
- Time server synchronization
- SNMP
- Email notification
- Read-only user access for web admin
- Shared IP drop-in mode
- Authentication and accounting by RADIUS server for web admin
- Built-in WINS servers*
- Syslog
- SIP passthrough
- PPTP packet passthrough
- Event log
- Active sessions
- Client list
- WINS client list *
- UPnP / NAT-PMP
- Real-time, hourly, daily, and monthly bandwidth usage reports and charts
- IPv6 support
- Support USB tethering on Android 2.2+ phones

* Not supported on MAX Surf-On-The-Go, and BR1 variants

2 BR2 Overview

2.1 Panel Appearance



2.1.1 LED Indicator

The statuses indicated by the front panel LEDs are as follows:

Status Indicator		
Status	OFF	System initializing/power off
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

3 Advanced Feature Summary

3.1 Drop-in Mode and LAN Bypass: Transparent Deployment



As your organization grows, it may require more bandwidth, but modifying your network can be tedious. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. For any reason your Peplink router loses power, the **LAN Bypass** will safely and automatically bypass the Peplink router to resume your original network connection.

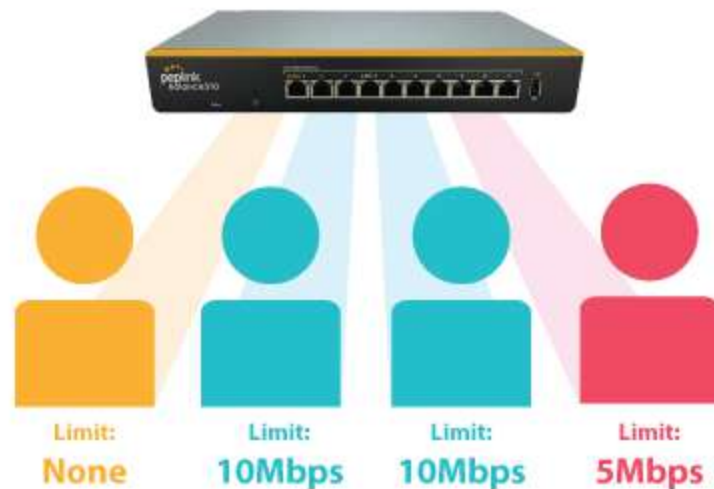
Note: Drop-in mode is compatible for All MAX models except MAX BR1 IP67

3.2 QoS: Clearer VoIP



VoIP and videoconferencing are highly sensitive to latency. With QoS, Peplink routers can detect VoIP traffic and assign it the highest priority, giving you crystal-clear calls.

3.3 Per-User Bandwidth Control



With per-user bandwidth control, you can define bandwidth control policies for up to 3 groups of users to prevent network congestion. Define groups by IP address and subnet, and set bandwidth limits for every user in the group.

3.4 High Availability via VRRP



When your organization has a corporate requirement demanding the highest availability with no single point of failure, you can deploy two Peplink routers in **High Availability mode**. With High Availability mode, the second device will take over when needed.

Compatible with: MAX 700, MAX HD2 (All variants), HD4 (All Variants)

3.5 USB Modem and Android Tethering



For increased WAN diversity, plug in a USB LTE modem as a backup. Peplink routers are compatible with over [200 modem types](#). You can also tether to smartphones running Android 4.1.X and above.

Compatible with: MAX 700, HD2 (all variants except IP67), HD4 (All variants)

3.6 Built-In Remote User VPN Support



Use OpenVPN or L2TP with IPsec to safely and conveniently connect remote clients to your private network. L2TP with IPsec is supported by most devices, but legacy devices can also connect using PPTP.

[Click here for the full instructions on setting up L2TP with IPsec.](#)

[Click here for the full instructions on setting up OpenVPN connections](#)

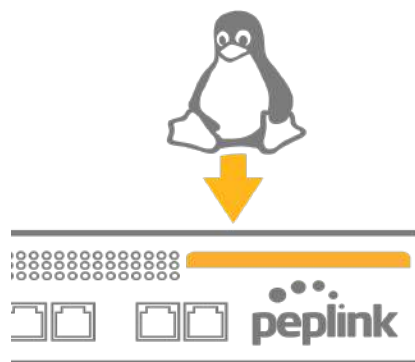
3.7 SIM-card USSD support



Cellular-enabled routers can now use USSD to check their SIM card's balance, process pre-paid cards, and configure carrier-specific services.

[Click here for full instructions on using USSD](#)

3.8 KVM Virtualization



KVM is a virtualisation module that allows administrators using our routers to host a large range of virtual machines. KVM is now supported on some MediaFast / ContentHub routers.

[Click here for the full instructions on how to set up KVM](#)

[Click here for the full instructions on how to set up KVM with USB Storage](#)

3.9 DPI Engine

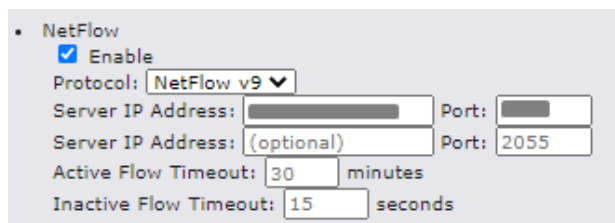
The DPI report written in the updated KB article will show further information on InControl2 through breaking down application categories into subcategories.

<https://forum.peplink.com/t/ic2-deep-packet-inspection-dpi-reports-and-everything-you-need-to-know-about-it/10151/>

3.10 NetFlow

NetFlow protocol is used to track network traffic. Tracking information from NetFlow can be sent to the NetFlow collector, which analyzes data and generates reports for review.

Note: To enable this feature, go to <https://<Device's IP>/cgi-bin/MANGA/support.cgi>



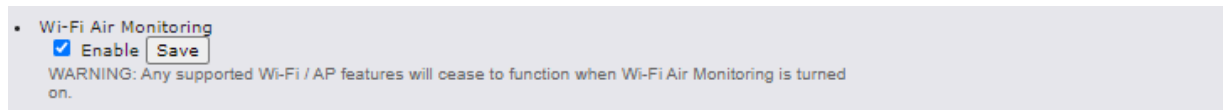
• NetFlow

- Enable
- Protocol:
- Server IP Address: Port:
- Server IP Address: Port:
- Active Flow Timeout: minutes
- Inactive Flow Timeout: seconds

3.11 Wi-Fi Air Monitoring

Pepwave routers support Wi-Fi “Air Monitoring Mode” which is used to troubleshoot remotely and proactively monitor Wi-Fi and WAN performance. The report can be viewed under InControl 2 > Reports > AirProbe Reports after enabling Wi-Fi Air Monitoring.

Note: To enable this feature, go to <https://<Device's IP>/cgi-bin/MANGA/support.cgi>



• Wi-Fi Air Monitoring

- Enable
- WARNING: Any supported Wi-Fi / AP features will cease to function when Wi-Fi Air Monitoring is turned on.

3.12 SP Default Configuration

The SP Default Configuration feature written in the updated KB article allows for the provisioning of custom made settings (a.k.a. InControl2 configuration) via the Ethernet LAN port and is ideal for those wanting to do a bulk deployment of many Peplink devices.

Note: If you would like to use this feature, please contact your purchase point (Eg. VAD).

3.13 Peplink Relay

Cloud Service Providers often restrict access to certain applications. With SFC Relay, you can route traffic before going out to the Internet, allowing access to previously restricted applications experienced with the public SpeedFusion Cloud nodes. Available as an add-on for your home router or as an upgradable license to your Peplink router, SFC Relay is sure to impress you and any peers you give access to.

<https://forum.peplink.com/t/configure-speedfusion-cloud-relay-server-and-client/6215ca9b017e48e0f3ff2479/>

3.14 DNS over HTTPS (DoH)

DoH provides the benefits of communicating DNS information over a secure HTTPS connection in an encrypted manner. The protocol offers increased privacy and confidentiality by preventing data interception and man-in-the-middle attacks.

3.15 Peplink InTouch

InTouch is Peplink's zero-touch remote network management solution, leveraging InControl 2 and a SpeedFusion Connect (formerly known as SpeedFusion Cloud) data plan. This service extends a network administrator's ability to reach any device UI backed by a Peplink/Pepwave router. To configure InTouch, all you need is a valid InControl 2 subscription, a SpeedFusion Connect data plan, and a Peplink/Pepwave router (which requires the latest 8.2.0 firmware).

To watch a demonstration and read the FAQ, visit

<https://www.peplink.com/enterprise-solutions/intouch/>

Or learn to configure InTouch at <https://youtu.be/zg0iavHGkJw>

3.16 Synergy Mode

Synergy mode is a cascade multiple devices and combine the number of WANs to a single device virtually. All the WANs on the Synergized Device will appear as native WAN interfaces at the Synergy Controller and it can be managed like the built-in WAN interfaces.

[https://forum.peplink.com/t/synergy-mode-\(firmware-8.3.0\)/639be7d8af8c71a6f3050323/](https://forum.peplink.com/t/synergy-mode-(firmware-8.3.0)/639be7d8af8c71a6f3050323/)

3.17 Virtual WAN on VLAN

The Virtual WAN Activation License allows you to create 1 x virtual WAN on a particular VLAN, on either WAN or LAN interface. This means that you can create a virtual WAN on VLAN for a WAN port, or a virtual WAN on VLAN for a LAN port.

<https://forum.peplink.com/t/b20x-virtual-wan-activation-license-faq/6204bac7d90b9e6355e96e8d/1>

4 Installation

The following section details connecting Pepwave routers to your network.

4.1 Preparation

Before installing your Pepwave router, please prepare the following as appropriate for your installation:

- At least one Internet/WAN access account and/or Wi-Fi access information
- Depending on network connection type(s), one or more of the following:
 - **Ethernet WAN:** A 10/100/1000BaseT UTP cable with RJ45 connector
 - **USB:** A USB modem
 - **Embedded modem:** A SIM card for 5G/4G LTE service
 - **Wi-Fi WAN:** Wi-Fi antennas
- A computer installed with the TCP/IP network protocol and a supported web browser. Supported browsers include Microsoft Internet Explorer 11 or above, Mozilla Firefox 24 or above, Apple Safari 7 or above, and Google Chrome 18 or above.

4.2 Constructing the Network

At a high level, construct the network according to the following steps:

1. With an Ethernet cable, connect a computer to one of the LAN ports on the Pepwave router. Repeat with different cables for up to 4 computers to be connected.
2. Connect either another Ethernet cable or a USB modem to one of the WAN ports or USB ports respectively, or connect to Wi-Fi as WAN on the Pepwave router. Repeat the same process for any additional WAN ports.
3. Connect the power adapter to the power connector on the rear panel of the Pepwave router, and then plug it into a power outlet.

4.3 Configuring the Network Environment

To ensure that the Pepwave router works properly in the LAN environment and can access the Internet via WAN connections, please refer to the following setup procedures:

- LAN configuration

For basic configuration, refer to **Section 8, Connecting to the Web Admin Interface**.

For advanced configuration, go to **Section 9, Configuring the LAN Interface(s)**.

- WAN configuration

For basic configuration, refer to **Section 8, Connecting to the Web Admin Interface**.

For advanced configuration, go to **Section 9.2, Captive Portal**.

5 Connecting to the Web Admin Interface

1. Start a web browser on a computer that is connected with the Pepwave router through the LAN.
2. To connect to the router's web admin interface, enter the following LAN IP address in the address field of the web browser:

http://192.168.50.1

(This is the default LAN IP address for Pepwave routers.)

3. Enter the following to access the web admin interface.

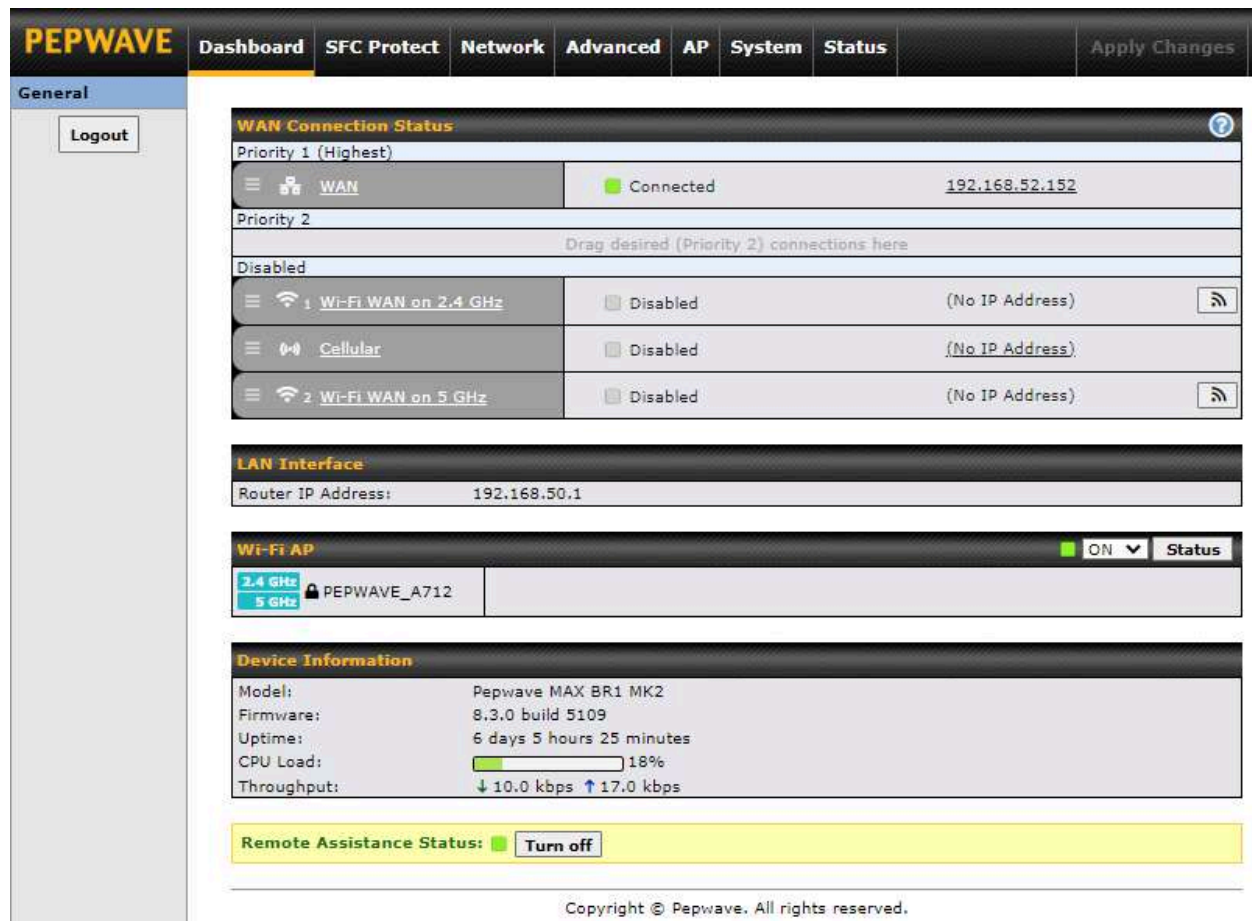
Username: admin

Password: admin

(This is the default username and password for Pepwave routers).

- You must change the default password on the first successful logon.
- Password requirements are: A minimum of 10 lower AND upper case characters, including at least 1 number.
- When HTTP is selected, the URL will be redirected to HTTPS by default.

After successful login, the **Dashboard** of the web admin interface will be displayed.



PEPWAVE Dashboard SFC Protect Network Advanced AP System Status Apply Changes

General Logout

WAN Connection Status

Priority 1 (Highest)

WAN	Connected	192.168.52.152
-----	-----------	----------------

Priority 2

Drag desired (Priority 2) connections here

Disabled

Wi-Fi WAN on 2.4 GHz	Disabled	(No IP Address)
Cellular	Disabled	(No IP Address)
Wi-Fi WAN on 5 GHz	Disabled	(No IP Address)

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP ON Status

2.4 GHz 5 GHz PEPWAVE_A712

Device Information

Model: Pepwave MAX BR1 MK2
 Firmware: 8.3.0 build 5109
 Uptime: 6 days 5 hours 25 minutes
 CPU Load: 18%
 Throughput: ↓ 10.0 kbps ↑ 17.0 kbps

Remote Assistance Status: Turn off

Copyright © Pepwave. All rights reserved.

The **Dashboard** shows current WAN, LAN, and Wi-Fi AP statuses. Here, you can change WAN connection priority and switch on/off the Wi-Fi AP. For further information on setting up these connections, please refer to **Sections 8** and **9**.

Device Information displays details about the device, including model name, firmware version, and uptime. For further information, please refer to **Section 22**.

Important Note

Configuration changes (e.g. WAN, LAN, admin settings, etc.) will take effect only after clicking the **Save** button at the bottom of each page. The **Apply Changes** button causes the changes to be saved and applied.

6 SpeedFusion Connect Protect

With Pepwave products, your device is able to connect to SpeedFusion Connect Protect without the use of a second endpoint. This service has wide access to a number of SpeedFusion endpoints hosted from around the world, providing your device with unbreakable connectivity wherever you are.*



*SpeedFusion Connect Protect is supported in firmware version 8.1.0 and above. SpeedFusion Connect is a subscription basis. SpeedFusion Connect Protect license can be purchased at <https://estore.peplink.com/> > **SpeedFusion Service** > **SpeedFusion Connect Protect**.

6.1 Activate SpeedFusion Connect Protect

All Care plans now come with SpeedFusion Connect Protect included. This data allowance will automatically begin and end in accordance with your warranty. No activation is required.

6.2 Enable SpeedFusion Connect Protect

Access the Web Admin of the device you want to create as the Peplink Relay Server, navigating to the “**SFC Protect**” tab.

The screenshot shows the Peplink Web Admin interface. The top navigation bar includes 'Dashboard', 'SFC Protect', 'Network', 'Advanced', 'AP', 'System', and 'Status'. The 'SFC Protect' tab is active. The main content area is titled 'SpeedFusion Connect Protect' and includes a sub-header 'Aggregate your bandwidth, connect you to different geo-location, and more.' Below this are three main sections: 'Get your activation key now', 'Client Mode - for Outbound accesses', and 'Relay Mode - for Inbound accesses'. Under 'Client Mode', there is a section for 'Outbound Traffic Steering Priority' with three options: 'Route by Cloud Application', 'Route by Wi-Fi SSID', and 'Route by LAN Client'. A 'Logout' button is visible in the left sidebar. At the bottom, there is a note: 'Click [here](#) to hide SpeedFusion Connect Protect menu, you can restore it later on Status page.'

To setup a Peplink Relay Mode, select “**Relay Mode - for Inbound accesses**” > Choose the **SFC Protect Location** you wish to connect to > Click on the **Green tick button** to confirm the change.

The screenshot shows the 'SpeedFusion Connect Protect > Setup Relay Mode' configuration screen. It includes a sub-header 'Allow remote peers to access local networks, and the internet via this device.' Below this is a table with two columns: 'SpeedFusion Connect Relay' and 'SFC Protect Location'. The 'SFC Protect Location' column contains a dropdown menu with 'Singapore (SIN) / 10ms' selected and a green checkmark button to the right. A help icon is visible in the top right corner of the table.

SpeedFusion Connect Relay	SFC Protect Location
	Singapore (SIN) / 10ms

The Relay Sharing Code will be generated, and other peers can use this code to establish a SpeedFusion Connect Protect that will forward the traffics to this device, allowing them to access local networks and the internet via your WAN connection.



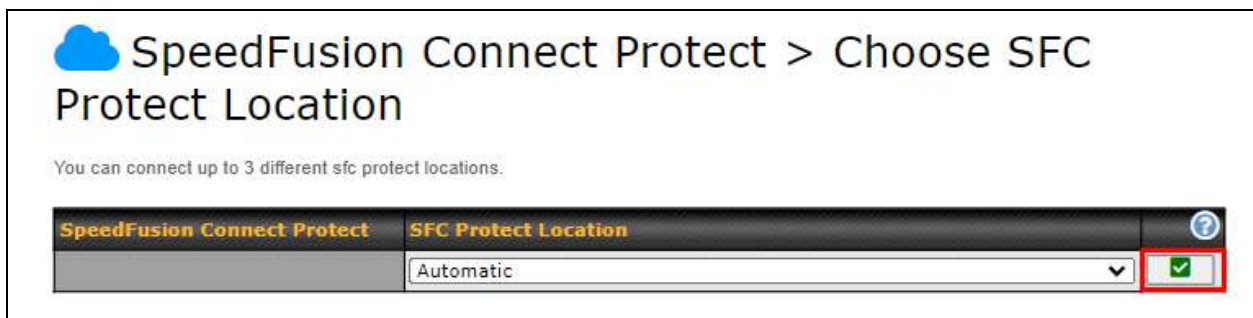
SpeedFusion Connect Protect > Setup Relay Mode

Allow remote peers to access local networks, and the internet via this device.

SpeedFusion Connect Relay	SFC Protect Location	
SFC-RELAY-SERVER-HKG	Relay Sharing Code: 7848-8886-6627-6299	<input type="checkbox"/>

To connect to SpeedFusion Connect Protect, you can select a **SFC Protect Location** of your choice, or simply and **Automatic** then the device will establish connection to the neareset SFC Protect server.

Choose **Automatic** > **Click on the green tick button** to confirm the change.



SpeedFusion Connect Protect > Choose SFC Protect Location

You can connect up to 3 different sfc protect locations.

SpeedFusion Connect Protect	SFC Protect Location	
	Automatic	<input checked="" type="checkbox"/>

Or you may select **Home Sharing** and use your **Relay Sharing Code** to create a profile if you have set up a Peplink Relay Client on another device.



SpeedFusion Connect Protect > Choose SFC Protect Location

You can connect up to 3 different sfc protect locations.

SpeedFusion Connect Protect	SFC Protect Location	
	[Relay Sharing] e.g. 1234-5678-1234-5678	<input checked="" type="checkbox"/>

Click on **Apply Changes** to save the change.

PEPWAVE Dashboard **SFC Protect** Network Advanced AP System Status **Apply Changes**

Saved! Changes will be effective after clicking the 'Apply Changes' button.

SpeedFusion Connect Protect > Choose SFC Protect Location

SpeedFusion Connect Protect	SFC Protect Location	
SFC	Automatic	X

By default, the router will build a SpeedFusion tunnel to the SpeedFusion Cloud.

Wi-Fi AP ON Status

No Wi-Fi AP

SpeedFusion Connect Protect

SFC	Established
-----	-------------

Data usage allowance:

If you are running a latency sensitive service like video streaming or VOIP, a WAN Smoothing sub-tunnel can be created. Navigate to **SFC Protect > Client Mode - for Outbound accesses > SFC**.

SpeedFusion Connect Protect > Choose SFC Protect Location

SpeedFusion Connect Protect	SFC Protect Location	
SFC	Automatic	X

A SpeedFusion Connect Protect Profile configuration window will pop out. Click on the + sign to create the WAN Smoothing sub-tunnel.

SpeedFusion Connect Protect Profile

Enable

SFC Protect Location Automatic

1 2 - WAN Smoo... **+**

Tunnel Options

Local / Remote Tunnel ID 2

Tunnel Name WAN Smoothing

Data Port Auto Custom

Bandwidth Limit

TCP Ramp Up

WAN Smoothing

Overall Redundancy Level	Normal
Maximum Level on the Same Link	Normal

Forward Error Correction Off

Receive Buffer 0 ms

Packet Fragmentation Always Use DF Flag

Click on **Save** and **Apply Changes** to save the configuration. Now, the router has 2 Speedfusion tunnels to the SpeedFusion Connect Protect.

Wi-Fi AP ON **Status**

No Wi-Fi AP

SpeedFusion Connect Protect

SFC (1)	<input checked="" type="checkbox"/> Established
SFC (2 - WAN Smoothing)	<input checked="" type="checkbox"/> Established

Data usage allowance:

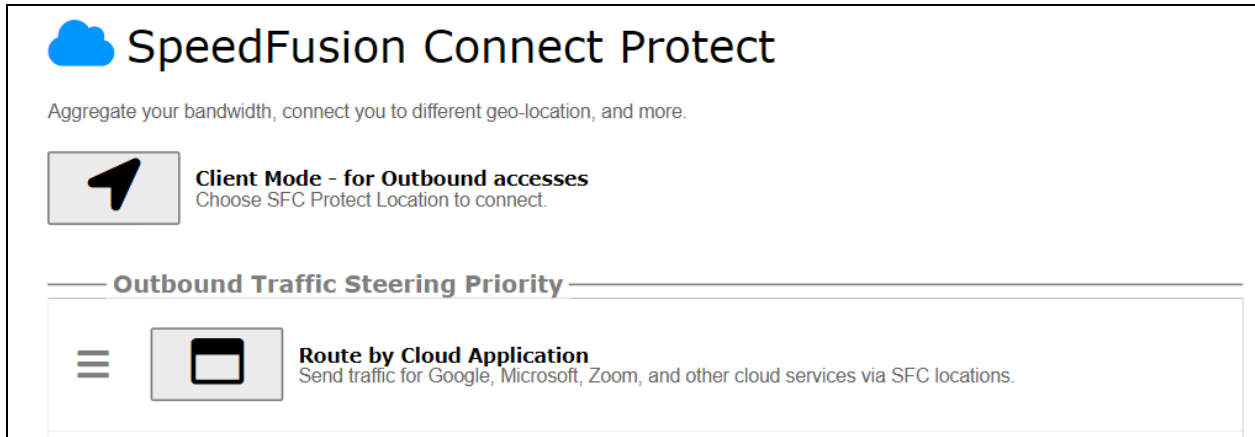
Create an outbound policy to steer the internet traffic to go into SFC Protect. Please go to **Advanced > Outbound Policy**, click on **Add Rule** to create a new outbound policy.

Rules (Drag and drop rows by the left to change rule order)

Service	Algorithm	Source	Destination	Protocol / Port	
PepVPN / OSPF / BGP / RIPv2 Routes SpeedFusion Cloud Routes					
to_internet	Priority VPN: SFC (1 - Def...	IP Address 192.168.50.10	Any	Any	✘
HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✘
Default	(Auto)				
Add Rule					

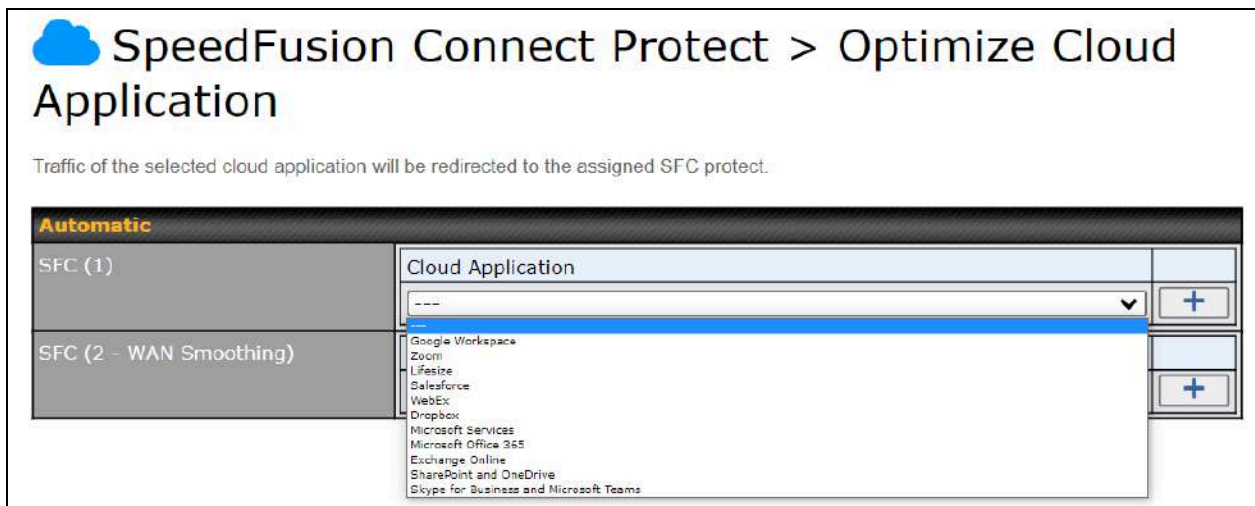
6.3 Route by Cloud Application

Optimize Cloud Application allows you to route Internet traffic through SpeedFusion Connect Protect based on the application. Go to **SFC Protect > Route by Cloud Application**.



Select a Cloud application to route through SpeedFusion Connect Protect from the drop down list > Click > Save > Apply Changes.

Click the to remove a selected Cloud application from routing through SpeedFusion Connect Protect.



6.4 Route by Wi-Fi SSID

SpeedFusion Connect Protect provides a convenient way to route the Wi-Fi client to the cloud from **SFC Protect > Route by Wi-Fi SSID**.

SpeedFusion Connect Protect
Aggregate your bandwidth, connect you to different geo-location, and more.

Client Mode - for Outbound accesses
Choose SFC Protect Location to connect.

Outbound Traffic Steering Priority

- Route by Cloud Application**
Send traffic for Google, Microsoft, Zoom, and other cloud services via SFC locations.
- Route by Wi-Fi SSID**
Send traffic via SFC locations by Wi-Fi SSID.

Create a new SSID for SFC Protect. The new SSID will inherit all settings from one of the existing SSIDs including the Security Policy. Then click **Save** followed by **Apply Changes**.

SpeedFusion Connect Protect > Link Wi-Fi to SFC Protect
The new SSID will inherit all settings from the existing SSID including the Security Policy.

Automatic			
SFC (1)	Reference SSID	SSID for SFC Protect	
	test-sfc	test-sfc (Automatic)	✖
	---		+
SFC (2 - WAN Smoothing)	Reference SSID	SSID for SFC Protect	
	---		+

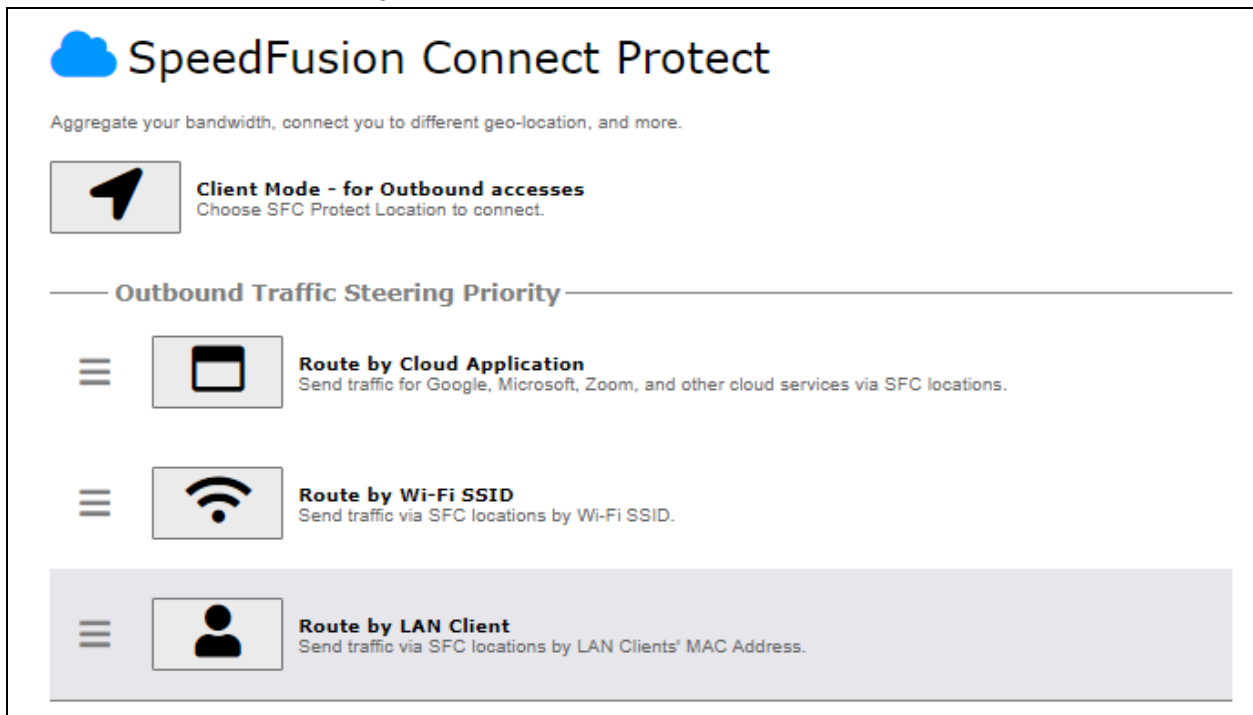
Save

SFC Protect SSID will be shown on **Dashboard**.



6.5 Route by LAN Client

SpeedFusion Connect Protect provides a convenient way to route the LAN client to the cloud from **SFC Protect > Route by LAN Client**.



Choose a client from the drop down list > Click + > Save > Apply Changes.

SpeedFusion Connect Protect > Connect Clients to SFC Protect

Traffic from the selected clients will be redirected to the assigned SFC protect.

Automatic			
SFC (1)	Client	IP Address	
	<input type="text" value=""/>	<input type="text" value=""/>	<input type="button" value="+"/>
SFC (2 - WAN Smoothing)	Client	IP Address	
	<input type="text" value="---"/>	<input type="text" value=""/>	<input type="button" value="+"/>

7 Configuring the LAN Interface(s)

7.1 Basic Settings

LAN interface settings are located at **Network > LAN > Network Settings**. Navigating to that page will show the following dashboard:

LAN	VLAN	Network	
LAN	None	172.16.251.1/24	
VLAN1	1	2.2.2.2/24	
VLAN2	2	3.3.3.3/24	

This represents the LAN interfaces that are active on your router (including VLAN). A gray “X” means that the VLAN is used in other settings and cannot be deleted. You can find which settings are using the VLAN by hovering over the gray “X”.

Alternatively, a red “X” means that there are no settings using the VLAN. You can delete that VLAN by clicking the red “X”

Clicking on any of the existing LAN interfaces (or creating a new one) will show the following :

IP Settings	
IP Address	<input type="text" value="255.255.255.0"/> (/24)

IP Settings	
IP Address	The IP address and subnet mask of the Pepwave router on the LAN.




Network Settings	
Name	<input type="text"/>
VLAN ID	<input type="text"/>
Inter-VLAN routing	<input checked="" type="checkbox"/>

Network Settings	
Name	Enter a name for the LAN.
VLAN ID	Enter a number for your VLAN
Inter-VLAN routing	Check this box to enable routing between virtual LANs.

Layer 2 SpeedFusion VPN Bridging		?
SpeedFusion VPN Profiles to Bridge	<input type="text" value="No profile is available"/>	Help Close If you want to enable DHCP Option 82 Injection, please click here . This allow the device to inject Option 82 with Device Name information before forwarding the DHCP Request packet to SpeedFusion VPN peer, such that the DHCP Server can identify where does this request come from.
Spanning Tree Protocol	<input type="checkbox"/>	
DHCP Option 82 Injection	<input checked="" type="checkbox"/>	
Override IP Address when bridge connected	<input checked="" type="radio"/> Do not override <input type="radio"/> Static <input type="radio"/> By DHCP <input type="radio"/> As None	

Layer 2 SpeedFusion VPN Bridging	
SpeedFusion VPN Profiles to Bridge	The remote network of the selected SpeedFusion VPN profiles will be bridged with this local LAN, creating a Layer 2 SpeedFusion VPN, they will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.
Spanning Tree Protocol	Click the box will enable STP for this layer 2 profile bridge.
DHCP Option 82	Click on the question Mark if you want to enable DHCP Option 82. This allows the device to inject Option 82 with Router Name information before forwarding the DHCP Request packet to a SpeedFusion VPN peer, such that the DHCP Server can identify where the request originates from.
Override IP Address when bridge connected	Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 SpeedFusion VPN is up. If you choose to override the IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.

DHCP Server									
DHCP Server	<input checked="" type="checkbox"/> Enable								
DHCP Server Logging	<input type="checkbox"/>								
IP Range	<input type="text"/> - <input type="text"/> <input type="text" value="255.255.255.0 (/24)"/> <input type="button" value="v"/>								
Lease Time	<input type="text" value="1"/> Days <input type="text" value="0"/> Hours <input type="text" value="0"/> Mins								
DNS Servers	<input checked="" type="checkbox"/> Assign DNS server automatically								
BOOTP	<input type="checkbox"/>								
Extended DHCP Option	<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;"><i>No Extended DHCP Option</i></td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Add"/></td> </tr> </tbody> </table>	Option	Value	<i>No Extended DHCP Option</i>		<input type="button" value="Add"/>			
Option	Value								
<i>No Extended DHCP Option</i>									
<input type="button" value="Add"/>									
DHCP Reservation	<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>00:00:00:00:00:00</td> <td></td> <td style="text-align: center;"><input type="button" value="+"/></td> </tr> </tbody> </table>	Name	MAC Address	Static IP			00:00:00:00:00:00		<input type="button" value="+"/>
Name	MAC Address	Static IP							
	00:00:00:00:00:00		<input type="button" value="+"/>						

DHCP Server Settings	
DHCP Server	<p>When this setting is enabled, the Pepwave router's DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collisions on the LAN.</p> <p>To enable DHCP bridge relay, please click the  icon on this menu item.</p>
DHCP Server Logging	Enable logging of DHCP events in the eventlog by selecting the checkbox.
IP Range	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of Lease Time , the assigned IP address will no longer be valid and the IP address assignment must be renewed.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If Assign DNS server automatically is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g. DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the Add button, choose the option to define, and then enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	<p>This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses.</p> <p>Name (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of 00:AA:BB:CC:DD:EE. Press  to create a new record. Press  to remove a record. Reserved clients information can be imported from the Client List, located at Status>Client List. For more details, please refer to Section 22.3.</p>

To configure DHCP relay, first click the button found next to the **DHCP Server** option to display the settings.

DHCP Relay Settings	
DHCP Relay	<input checked="" type="checkbox"/> Enable
DHCP Server IP Address	DHCP Server 1: <input type="text"/> DHCP Server 2: <input type="text"/>
DHCP Option 82	<input type="checkbox"/>
DHCP Relay Logging	<input type="checkbox"/>

DHCP Relay Settings	
Enable	Check this box to turn on DHCP relay. Click the icon to disable DHCP relay.
DHCP Server IP Address	Enter the IP addresses of one or two DHCP servers in the provided fields. The DHCP servers entered here will receive relayed DHCP requests from the LAN. For active-passive DHCP server configurations, enter active and passive DHCP server relay IP addresses in DHCP Server 1 and DHCP Server 2 .
DHCP Option 82	DHCP Option 82 includes device information as relay agent for the attached client when forwarding DHCP requests from client to server. This option also embeds the device's MAC address and network name in circuit and remote IDs. Check this box to enable DHCP Option 82.
DHCP Relay Logging	Enable logging of DHCP Relay events in the eventlog by selecting the checkbox.

Once DHCP is set up, configure **LAN Physical Settings**, **Static Route Settings**, and **DNS Proxy Settings** as noted above.

Static Route Settings			
Static Route	Destination Network	Subnet Mask	Gateway
		255.255.255.0 (/24) ▼	

Static Route Settings	
Static Route	<p>This table is for defining static routing rules for the LAN segment. A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in w.x.y.z format.</p> <p>The local LAN subnet and subnets behind the LAN will be advertised to the VPN. Remote routes sent over the VPN will also be accepted. Any VPN member will be able to route to the local subnets. Press to create a new route. Press to remove a route.</p>

^A - Advanced feature, please click the button on the top right hand corner of the Static Route section to activate and configure Virtual Network Mapping to resolve network address conflict with remote peers.

Virtual Network Mapping ?			
One-to-One NAT ?	Local Network ?	Virtual Network	+
	▼		
Many-to-One NAT ?	Local Network ?	Virtual IP Address	+
	▼		

In case of a network address conflict with remote peers (i.e. SpeedFusion VPN / IPsec VPN / IP Forwarding WAN are considered as remote connections), you can define Virtual Network Mapping to resolve it.

Note: OSPF & RIPv2 settings should be updated as well to avoid advertising conflicted networks.

For further details on virtual network mapping watch this video:

<https://youtu.be/C1FMdZCn3Z8>

Virtual Network Mapping	
One-to-One NAT	<p>Every IP Address in the Local Network has a corresponding unique Virtual IP Address for NAT.</p> <p>Traffic originating from the Local Network to remote connections will be SNAT'ed and behave like coming from the defined Virtual Network.</p> <p>While traffic initiated by remote peers to the Virtual Network will be DNAT'ed accordingly.</p>
Many-to-One NAT	<p>The subnet range defined in Local Network will be mapped to a single Virtual IP Address for NAT. Traffic can only be initiated from local to remote, and these traffic will be NAT'ed and behaves like coming from the same Virtual IP Address.</p>

DNS Proxy Settings ?			
Enable	<input checked="" type="checkbox"/>		
DNS Caching ?	<input type="checkbox"/>		
Include Google Public DNS Servers ?	<input type="checkbox"/>		
Local DNS Records ?	Host Name	IP Address	TTL
	<input type="text"/>	<input type="text"/>	3600 <input type="button" value="+"/>
Domain Lookup Policy ?	Domain	Connection	<input type="button" value="+"/>
	<input type="text"/>	<input type="text" value="v"/>	
DNS Resolvers ?	<input type="checkbox"/> WAN	192.168.52.1	
	<input type="checkbox"/> Cellular		
	<input type="checkbox"/> Wi-Fi WAN on 2.4 GHz		
	<input type="checkbox"/> Wi-Fi WAN on 5 GHz		
	<input type="checkbox"/> SFC	<input type="text"/>	
	<input type="checkbox"/> Untagged LAN	<input type="text"/>	
Preferred connections are shown with <input checked="" type="checkbox"/>			
<input type="button" value="Save"/>			


DNS Proxy Settings	
Enable	To enable the DNS proxy feature, check this box, and then set up the feature at Network > LAN > DNS Proxy Settings . A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the DNS servers/resolvers defined for each WAN connection.
DNS Caching	This field is to enable DNS caching on the built-in DNS proxy server. When the option is enabled, queried DNS replies will be cached until the records' TTL has been reached. This feature can help improve DNS lookup time. However, it cannot return the most up-to-date result for those frequently updated DNS records. By default, DNS Caching is disabled.
Include Google Public DNS Servers	When this option is enabled , the DNS proxy server will also forward DNS requests to Google's Public DNS Servers, in addition to the DNS servers defined in each WAN. This could increase the DNS service's availability. This setting is disabled by default.
Local DNS Records	This table is for defining custom local DNS records. A static local DNS record consists of a host name and IP address. When looking up the host name from the LAN to LAN IP of the Pepwave router, the corresponding IP address will be returned. Press <input type="button" value="+"/> to create a new record. Press <input type="button" value="x"/> to remove a record.
Domain Lookup Policy	DNS Proxy will lookup the domain names defined in this table using the specified connections only.

DNS Resolvers ^A



This field specifies which DNS servers can receive forwarded DNS requests. If no DNS server is selected, then all of them will be selected by default.

If you wish to select a SpeedFusion VPN peer, enter the IP address(es) of the VPN peer's DNS server.

Incoming queries will be forwarded to one of the selected servers. If none of the selected servers can be reached, then the router will forward incoming queries to all servers with healthy WAN connections.

^A - Advanced feature, please click the  button on the top right hand corner to activate.

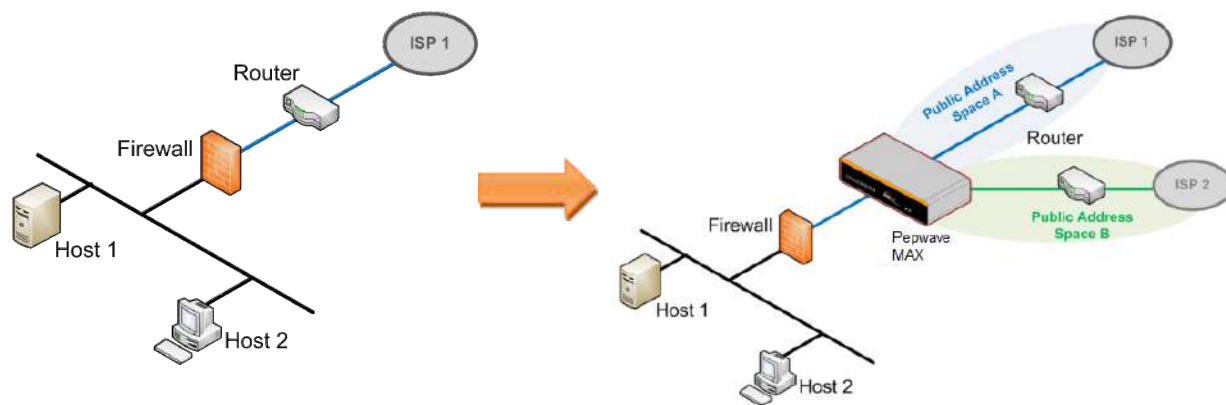
Finally, if needed, configure Bonjour forwarding, Apple's zero configuration networking protocol. Once VLAN configuration is complete, click **Save** to store your changes.

Bonjour Forwarding Settings	
Enable	Check this box to turn on Bonjour forwarding.
Bonjour Service	Choose Service and Client networks from the drop-down menus, and then click  to add the networks. To delete an existing Bonjour listing, click  .

Drop-In Mode

Drop-in mode (or transparent bridging mode) eases the installation of the Pepwave MAX on a live network between the firewall and router, such that changes to the settings of existing equipment are not required.

The following diagram illustrates drop-in mode setup:



Check the box Enable to enable the Drop-in Mode. After enabling this feature and selecting the WAN for Drop-in mode, various settings including the WAN's connection method and IP address will be automatically updated.


When drop-in mode is enabled, the LAN and the WAN for drop-in mode ports will be bridged. Traffic between the LAN hosts and WAN router will be forwarded between the devices. In this case, the hosts on both sides will not notice any IP or MAC address changes.


After successfully setting up the Pepwave MAX as part of the network using drop-in mode, it will, depending on model, support one or more WAN connections. Some MAX units also support multiple WAN connections after activating drop-in mode, though a SpeedFusion license may be required to activate more than one WAN port.

Please note the Drop-In Mode is mutually exclusive with VLAN.

Drop-In Mode Settings ?							
Enable	<input checked="" type="checkbox"/>						
WAN for Drop-In Mode ?	WAN ▼ <input checked="" type="checkbox"/> Apply NAT on VLAN networks outgoing Internet traffic VLAN network(s) may route their outgoing Internet traffic to this unit. When this checkbox is checked their traffic will be NAT'd before forwarding out of this WAN. Leave this checkbox checked if you are not sure.						
Share Drop-In IP ?	<input checked="" type="checkbox"/>						
Shared IP Address ?	<input type="text"/> 255.255.255.0 (/24) ▼						
Static Route	<table border="1" style="width: 100%;"> <thead> <tr> <th>Destination Network</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24) ▼</td> <td style="text-align: center;">+</td> </tr> </tbody> </table>	Destination Network	Subnet Mask		<input type="text"/>	255.255.255.0 (/24) ▼	+
Destination Network	Subnet Mask						
<input type="text"/>	255.255.255.0 (/24) ▼	+					
WAN Default Gateway ?	<input type="text"/> <input checked="" type="checkbox"/> I have other host(s) on WAN segment IP Address <input type="text"/> - <input type="text"/> <div style="text-align: center;">↓</div> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="text-align: right;">✕</div>						
WAN DNS Servers ?	DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>						
<p>NOTE: The DHCP Server Settings will be overwritten.</p> <p>The following WAN settings will be overwritten: Connection Method, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.</p> <p>The PPTP Server will be disabled.</p> <p>Tip: please review the DNS Forwarding setting under the Service Forwarding section.</p>							

Drop-in Mode Settings	
Enable	Drop-in mode eases the installation of the Pepwave MAX on a live network between the existing firewall and router, such that no configuration changes are required on existing equipment. Check the box to enable the drop-in mode feature.
WAN for Drop-In Mode	Select the WAN port to be used for drop-in mode. If WAN is selected, the high availability feature will be disabled automatically.
Shared Drop-In IP^A	<p>When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The MAX will listen for this IP address when WAN hosts access services provided by the MAX (web admin access from the WAN, DNS server requests, etc.).</p> <p>To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The MAX will listen for this IP address when LAN hosts access services provided by the MAX (web admin access from the WAN, DNS proxy, etc.).</p>

Shared IP Address^A	Access to this IP address will be passed through to the LAN port if this device is not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (e.g., email notification, remote syslog, etc.) The device will also listen on the IP address when hosts on the WAN access services served on this device (e.g., web admin accesses from WAN, DNS server, etc.)
WAN Default Gateway	Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the WAN segment, click the  button next to "WAN Default Gateway" and check the other host(s) on the WAN segment box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.
WAN DNS Servers	Enter the selected WAN's corresponding DNS server IP addresses.

^A - Advanced feature, please click the  button on the top right-hand corner to activate.

7.2 Port Settings

To configure port settings, navigate to **Network > Port Settings**

Port Settings					
Port Name	Enable	Speed	Advertise Speed	Port Type	VLAN
LAN Port 1	<input checked="" type="checkbox"/>	Auto <input type="text"/>	<input checked="" type="checkbox"/>	Trunk <input type="text"/>	Any <input type="text"/>
LAN Port 2	<input checked="" type="checkbox"/>			Trunk <input type="text"/>	Any <input type="text"/>
LAN Port 3	<input checked="" type="checkbox"/>			Trunk <input type="text"/>	Any <input type="text"/>
LAN Port 4	<input checked="" type="checkbox"/>			Trunk <input type="text"/>	Any <input type="text"/>

On this screen, you can enable specific ports, as well as determine the speed of the LAN ports, whether each port is a trunk or access port, can well as which VLAN each link belongs to, if any.

7.3 Captive Portal

The captive portal serves as a gateway that clients have to pass if they wish to access the internet using your router. To configure, navigate to **Network > LAN > Captive Portal**.

Captive Portal
✕

General Settings

Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Untagged LAN
Hostname ?	<input type="text"/> Default
Access Mode	<input checked="" type="radio"/> Open Access <input type="radio"/> User Authentication <input type="radio"/> External Server

Portal Access Settings

Access Quota	<input type="text" value="30"/> mins (0: Unlimited) <input type="text" value="0"/> MB (0: Unlimited)				
Quota Reset Time	<input checked="" type="radio"/> Daily at <input type="text" value="00"/> :00 <input type="radio"/> <input type="text" value="1440"/> minutes after quota reached				
Inactive Timeout	<input type="text" value="0"/> minutes (0: No Timeout)				
Allowed Networks ?	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="font-size: small;">Domain Name / IP Address / Network</td> <td style="width: 30px; text-align: center;">+</td> </tr> <tr> <td><input type="text"/></td> <td style="text-align: center;">+</td> </tr> </table>	Domain Name / IP Address / Network	+	<input type="text"/>	+
Domain Name / IP Address / Network	+				
<input type="text"/>	+				
Allowed Clients	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="font-size: small;">MAC / IP Address / Host Identifier</td> <td style="width: 30px; text-align: center;">+</td> </tr> <tr> <td><input type="text"/></td> <td style="text-align: center;">+</td> </tr> </table>	MAC / IP Address / Host Identifier	+	<input type="text"/>	+
MAC / IP Address / Host Identifier	+				
<input type="text"/>	+				
Splash Page ?	<input checked="" type="radio"/> Built-in <input type="radio"/> External, URL: <input type="text" value="http://"/>				
Popup Handling	<input type="checkbox"/> Bypass Popup (Redirection only takes place on normal browser) <input type="checkbox"/> Automatically show splash page on Safari for Apple (iOS / macOS) devices				
Logout Hostname ?	<input type="text" value="(Not configured)"/>				

Click [here](#) to preview / customize built-in splash page

Save
Cancel

Captive Portal Settings	
Name	Enter the name for the Captive Portal.
Enable	Check Enable and then, optionally, select the LANs/VLANs that will use the captive portal.
Hostname	To customize the portal's form submission and redirection URL, enter a new URL in this field. To reset the URL to factory settings, click Default .

Access Mode

Click **Open Access** to allow clients to freely access your router. Click **User Authentication** to force your clients to authenticate before accessing your router.

Select **External Server** to use the Captive Portal with a HotSpot system.

As described in the following knowledgebase article:

<https://forum.peplink.com/t/using-hotspotsystem-wi-fi-on-pepwave-max-routers/>

Authentication

When selecting the “**User Authentication**” in the Access Mode field, you will see the available option for the Authentication via drop-down list:

- RADIUS Server

Access Mode	<input type="radio"/> Open Access <input checked="" type="radio"/> User Authentication <input type="radio"/> External Server	
Authentication	RADIUS Server ▼	
RADIUS Settings		
	Primary	Secondary
Authentication Protocol	PAP ▼	
	You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server page to define multiple profiles	
Authentication Host	<input type="text"/>	<input type="text"/>
Authentication Port	1812	1812
Authentication Secret	<input type="text"/>	<input type="text"/>
	<input checked="" type="checkbox"/> Hide Characters	<input checked="" type="checkbox"/> Hide Characters
	You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server page to define multiple profiles	
Accounting Host	<input type="text"/>	<input type="text"/>
Accounting Port	1813	1813
Accounting Secret	<input type="text"/>	<input type="text"/>
	<input checked="" type="checkbox"/> Hide Characters	<input checked="" type="checkbox"/> Hide Characters
CoA-DM	<input type="checkbox"/>	
Accounting Interim Interval	<input type="text"/>	
NAS-Identifier	Device Name ▼	

- LDAP Server

Access Mode	<input type="radio"/> Open Access <input checked="" type="radio"/> User Authentication <input type="radio"/> External Server	
Authentication	LDAP Server ▼	
LDAP Settings		
LDAP Server	<input type="text"/>	Port <input type="text"/> <input type="button" value="Default"/>
	<input type="checkbox"/> Use DN/Password to bind to LDAP Server	
Base DN	<input type="text"/>	
Base Filter	<input type="text"/>	

Fill in the necessary information to complete your connection to the server and enable authentication.

External Server

When selecting the “**External Server**” in the Access Mode field, you will see the available option for the Service Type via drop-down list:

- CoovaChilli

	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Access Mode <input type="radio"/> Open Access <input type="radio"/> User Authentication <input checked="" type="radio"/> External Server</p> <p>Server Type ? CoovaChilli ▼</p> <hr/> <p>CoovaChilli Settings</p> <p>UAM Secret <input type="text"/> <input checked="" type="checkbox"/> Hide Characters</p> </div> <ul style="list-style-type: none"> • HotspotSystem <div style="border: 1px solid #ccc; padding: 5px;"> <p>Access Mode <input type="radio"/> Open Access <input type="radio"/> User Authentication <input checked="" type="radio"/> External Server</p> <p>Server Type ? HotspotSystem ▼</p> <hr/> <p>HotspotSystem Settings</p> <p>Operator Username <input type="text"/></p> <p>Location ID <input type="text"/></p> <p>Splash Page Domain ? customer.hotspotsystem.com</p> </div> <p>Fill in the necessary information to complete your connection to the server and enable authentication.</p>
Access Quota	Set a time and data cap to each user's Internet usage.
Quota Reset Time	This menu determines how your usage quota resets. Setting it to Daily will reset it at a specified time every day. Setting a number of minutes after quota reached establish a timer for each user that begins after the quota has been reached.
Inactive Timeout	Clients will get disconnected when the inactive the configured time is reached. Default 0: no timeout
Allowed Networks	Add networks that can bypass the captive Portal in this field. To whitelist a network, enter the domain name / IP address here and click + . To delete an existing network from the list of allowed networks, click the ✖ button next to the listing.
Allowed Clients	Add MAC address and /or IP addresses for client devices that are allowed to bypass the Captive Portal. Clients accessing these domains and IP addresses will not be redirected to the splash page.
Splash Page	Here, you can choose between using the Pepwave router's built-in captive portal and redirecting clients to a URL you define.
Popup Handling	Configurable options for popup handling: - Bypass Popup (Redirection only takes place on normal browser) - Automatically show splash page on Safari for Apple (iOS / macOS) devices
Logout Hostname	A hostname that can be used to logout captive portal when being accessed on browser.
Customize splash page	Click on the provided link in the Captive portal profile to customize the splash page. A new browser tab is opened with a WYSIWYG editor of the splash page o edit the content, click on the corresponding element after switching Edit Mode to ON.

Captive Portal



Use uploaded Logo Image
 Use default Logo Image
 No file chosen

NOTE: Size max 512KB. Supported images types: JPEG, PNG and GIF.

EMPTY STRING

I have read and agree to the [terms and conditions](#) ?

You must accept the terms and conditions before you can proceed

Agree

Powered by Pepwave.

Portal Configuration

Show Quota Status	<input checked="" type="checkbox"/>
Custom Landing Page	<input type="checkbox"/>

Page: v

Edit mode ON ?

Save

8 Configuring the WAN Interface(s)

WAN Interface settings are located at **Network > WAN**. To reorder WAN priority, drag on the appropriate WAN by holding the left mouse button, move it to the desired priority (the first one would be the highest priority, the second one would be lower priority, and so on), and drop it by releasing the mouse button.

The screenshot shows the Peplink PEPWAVE web interface. The top navigation bar includes: PEPWAVE, Dashboard, SFC Protect, Network, Advanced, AP, System, Status, and Apply Changes. The left sidebar has a Logout button. The main content area is divided into several sections:

- WAN Connection Status:** Shows Priority 1 (Highest) with a 'WAN' connection that is 'Connected'. Below it, Priority 2 is empty with the instruction 'Drag desired (Priority 2) connections here'. Under the 'Disabled' section, there are three options: 'Cellular' (Disabled, No IP Address), 'Wi-Fi WAN on 2.4 GHz' (Disabled, No IP Address), and 'Wi-Fi WAN on 5 GHz' (Disabled, No IP Address).
- LAN Interface:** Shows Router IP Address: 192.168.50.1.
- Wi-Fi AP:** Shows status as 'ON' and a 'Status' button. Below it are '2.4 GHz' and '5 GHz' options with a lock icon and the text 'PEPWAVE'.
- Device Information:** Lists Model: Pepwave MAX BR1 MK2, Firmware: 8.3.0 build 5109, Uptime: 6 days 8 hours 28 minutes, CPU Load: 16% (with a progress bar), and Throughput: ↓ 9.0 kbps ↑ 32.0 kbps.
- Remote Assistance Status:** Shows a green indicator and a 'Turn off' button.

At the bottom, there is a copyright notice: Copyright © Pepwave. All rights reserved.

To enable a particular WAN connection, drag on the appropriate WAN by holding the left mouse button, move it to the **Disabled** row, and drop it by releasing the mouse button.

You can also set priorities on the **Dashboard**. Click the **WAN** button in the corresponding row to modify the connection setting.

Important Note

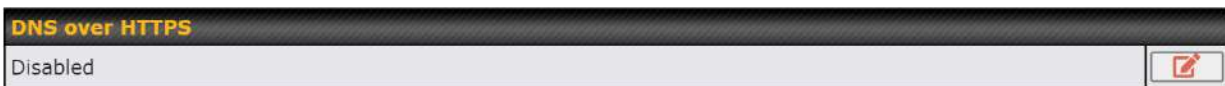
Connection details will be changed and become effective immediately after clicking the **Save and Apply** button.

IPv6

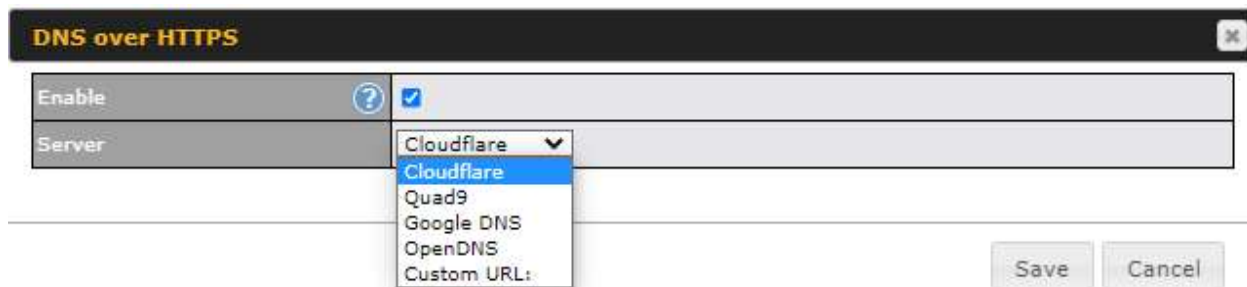


You can also enable IPv6 support in this section.

DNS over HTTPS (DoH)



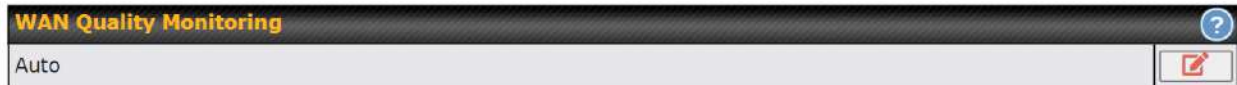
You can enable DoH (DNS over HTTPS) support in this section.



DNS over HTTPS	
Enable	When this option is enabled, the DNS proxy server will use HTTPS connections to forward DNS requests to the DoH resolver; it will not fallback to traditional UDP DNS options.
Server	<p>The options to configure DoH with a predefined server are:</p> <ul style="list-style-type: none"> • Cloudflare - The DNS server IP addresses for Cloudflare will be using 1.1.1.1, which is unfiltered. • Quad9 - The DNS server IP addresses for Quad9 will be using 9.9.9.9 and 142.112.112.112, which is malware blocking and DNSSEC. • Google DNS - The DNS server IP addresses for Google DNS will be using 8.8.8.8 and 8.8.4.4, which is RFC8484 standard. • OpenDNS - The DNS server IP addresses for OpenDNS will be using 208.67.222.222 and 208.67.220.220, which is standard DNS. • Custom URL - You may select Custom URL:, and enter the resolver URL and IP address.

WAN Quality Monitoring

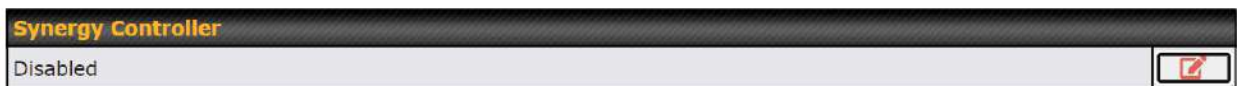
This settings advice how WAN Quality information is being gathered.



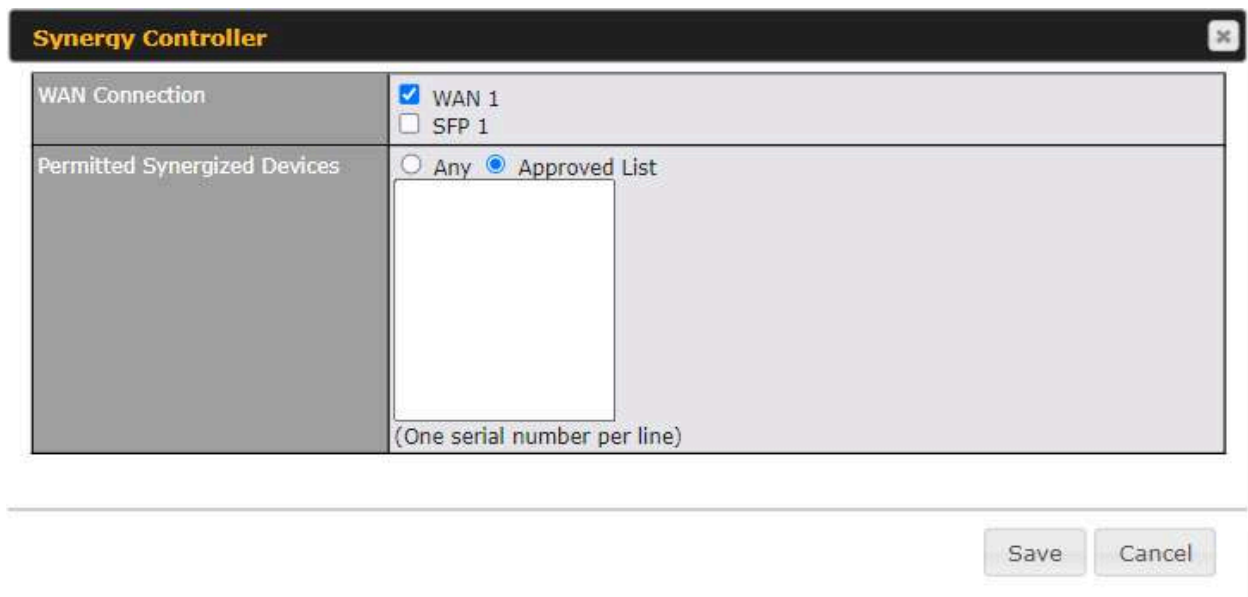
By default, WAN Quality will always be observed and gathered automatically. With customized choice of WAN connections, the device will always observe WAN Quality of those selected WAN connections. Other WAN connections may stop observing WAN Quality information if it is not necessary for the underlying features.

Synergy Mode

You can enable the Synergy Controller in this section.



You may click this  to enable the Synergy Controller. By default, the setting is disabled.



You may select the WAN connection to use as a Synergy Link which will connect to synergized devices.

8.1 Ethernet WAN

There are four possible connection methods for the Ethernet WAN connection:


1. DHCP
2. Static IP
3. PPPoE
4. L2TP
5. GRE

8.1.1 DHCP Connection

The DHCP connection method is suitable if the ISP provides an IP address automatically using DHCP (e.g., satellite modem, WiMAX modem, cable, Metro Ethernet, etc.).

WAN Connection Settings	
WAN Connection Name	WAN
Enable	<input checked="" type="checkbox"/>
Connection Priority	<input checked="" type="radio"/> Always-on (Priority 1) <input type="radio"/> Backup
Independent from Backup WANs	<input type="checkbox"/>
Connection Method	DHCP
Routing Mode	<input checked="" type="radio"/> NAT <input type="radio"/> IP Forwarding
Management IP Address	255.255.255.0 (/24)
Custom Hostname	<input type="checkbox"/>
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>
IP Passthrough	<input type="checkbox"/>
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Reply to ICMP Ping	<input checked="" type="radio"/> Yes <input type="radio"/> No
Upload Bandwidth	1 Gbps
Download Bandwidth	1 Gbps




DHCP Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Enable	This setting enables the WAN connection. If schedules have been defined, you will be able to select a schedule to apply to the connection.

<p>Connection Priority</p>	<p>This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only.</p> <p>If Always-on is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections.</p> <p>If Backup is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.</p>
<p>Independent from Backup WANs</p>	<p>If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.</p>
<p>Routing Mode</p>	<p>NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help  icon in this field, you can display the IP Forwarding option, if your network requires it.</p>
<p>Management IP Address</p>	<p>Management IP Address is available for configuration when you click here for other DHCP settings.</p> <p>This option allows you to configure the management IP address for the DHCP WAN connection.</p>
<p>Custom Hostname</p>	<p>If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with the value, you can safely bypass this option.</p>
<p>DNS Servers</p>	<p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.)</p> <p>When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS Server 1 and DNS Server 2 fields.</p>

<p>IP Passthrough</p>	<p>When this IP Passthrough option is active, after the ethernet WAN connection is up, the router's DHCP server will offer the connection's IP address to one LAN client. All incoming or outgoing traffic will be routed without NAT.</p> <p>Regardless the WAN connection's state, the router always binds to the LAN IP address (Default: 192.168.50.1). So when the ethernet WAN is connected, the LAN client could access the router's web admin by manually configuring its IP address to the same subnet as the router's LAN IP address (e.g. 192.168.50.10).</p> <p>Note: when this option is firstly enabled, the LAN client may not be able to refresh its IP address to the ethernet WAN IP address in a timely fashion. The LAN client may have to manually renew its IP address from DHCP server. After this option is enabled, the DHCP lease time will be 2 minutes. I.e. the LAN client could refresh its IP address and access the network at most one minute after the ethernet WAN connection goes up.</p>
<p>Standby State</p>	<p>This option allows you to choose whether to remain connected when this WAN connection is no longer in the highest priority and has entered the standby state. When Remain connected is chosen, upon bringing up this WAN connection to active, it will be immediately available for use.</p> <p>If this WAN connection is charged by connection time, you may want to set this option to Disconnect so that connection will be made only when needed.</p> <p>SpeedFusion VPN may use connected standby WAN for failover if link failure detected on the higher priority WAN, you can set this option to Disconnect to avoid data passing through.</p>
<p>Reply to ICMP PING</p>	<p>If the checkbox is unticked, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection.</p> <p>Default: ticked (Yes)</p>
<p>Upload Bandwidth</p>	<p>This field refers to the maximum upload speed.</p> <p>This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. A correct value can result in effective traffic prioritization and efficient use of upstream bandwidth.</p>
<p>Download Bandwidth</p>	<p>This field refers to the maximum download speed.</p> <p>Default weight control for outbound traffic will be adjusted according to this value.</p>

8.1.2 Static IP Connection






The Static IP connection method is suitable if your ISP provides a static IP address to connect directly.

Connection Method	 Static IP ▼
Routing Mode	 <input checked="" type="radio"/> NAT <input type="radio"/> IP Forwarding
IP Address	 <input type="text"/>
Subnet Mask	255.255.255.0 (/24) ▼
Default Gateway	<input type="text"/>
DNS Servers	<input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

Static IP Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the IP Forwarding option, if your network requires it.
IP Address / Subnet Mask / Default Gateway	These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address. The information is typically determined by and can be obtained from the ISP.
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.</p> <p>When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS Server 1 and DNS Server 2 fields.</p>

8.1.3 PPPoE Connection

The PPPoE connection method is suitable if your ISP provides a login ID/password to connect via PPPoE.

Connection Method	 PPPoE ▼
Routing Mode	 <input checked="" type="radio"/> NAT <input type="radio"/> IP Forwarding
PPPoE User Name	<input type="text"/>
PPPoE Password	<input type="password"/>
Confirm PPPoE Password	<input type="password"/>
Service Name (Optional)	<input type="text"/> Leave it blank unless it is provided by ISP
IP Address (Optional)	 <input type="text"/> Leave it blank unless it is provided by ISP
Keep-Alive Interval	 <input type="text" value="6"/> seconds(s)
Keep-Alive Retry	 <input type="text" value="6"/>
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

PPPoE Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the IP Forwarding option, if your network requires it.
PPPoE Username / Password	Enter the required information in these fields in order to connect via PPPoE to the ISP. The parameter values are determined by and can be obtained from the ISP.
Confirm PPPoE Password	Verify your password by entering it again in this field.
Service Name (Optional)	Service name is provided by the ISP. Note: Leave this field blank unless it is provided by your ISP.
IP Address (Optional)	If your ISP provides a PPPoE IP address, enter it here. Note: Leave this field blank unless it is provided by your ISP.
Keep Alive Interval	This is the time interval between each Keep-Alive packet.
Keep-Alive Retry	This is the number of consecutive Keep-Alive check failures before treating PPPoE connection as down.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.

Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.)

When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

8.1.4 L2TP Connection

L2TP has all the compatibility and convenience of PPTP with greater security. Combine this with IPsec for a good balance between ease of use and security.

Connection Method	<input data-bbox="527 793 560 835" type="button" value="?"/> L2TP <input data-bbox="673 793 706 835" type="button" value="v"/>
Routing Mode	<input data-bbox="527 840 560 882" type="button" value="?"/> <input checked="" type="radio"/> NAT <input type="radio"/> IP Forwarding
L2TP User Name	<input type="text"/>
L2TP Password	<input type="password"/>
Confirm L2TP Password	<input type="password"/>
Server IP Address / Host	<input type="text"/>
Address Type	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

L2TP Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the IP Forwarding option, if your network requires it.
L2TP Username / Password	Enter the required information in these fields in order to connect via L2TP to your ISP. The parameter values are determined by and can be obtained from your ISP.
Confirm L2TP Password	Verify your password by entering it again in this field.
Server IP Address / Host	L2TP server address is a parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP.
Address Type	Your ISP will also indicate whether the server IP address is Dynamic or Static. Please click the appropriate value.

DNS Servers

Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.



Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection.

(The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.)

When **Use the following DNS server address(es)** is selected, you can enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.

8.1.5 GRE Connection

This connection method is suitable if your ISP provides a static WAN IP and Tunnel IP via GRE.

Connection Method	 GRE ▼
Routing Mode	 <input checked="" type="radio"/> NAT <input type="radio"/> IP Forwarding
WAN IP Address	<input type="text"/>
WAN Subnet Mask	255.255.255.0 (/24) ▼
WAN Default Gateway	<input type="text"/>
Remote GRE Host	<input type="text"/>
Tunnel Local IP Address	<input type="text"/>
Tunnel Remote IP Address	<input type="text"/>
Outgoing NAT IP Address	<input type="text"/>
DNS Servers	<input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

GRE Settings

Routing Mode

NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.

WAN IP Address / Subnet Mask / Default Gateway

These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address. The information is typically determined by and can be obtained from the ISP.

Remote GRE Host

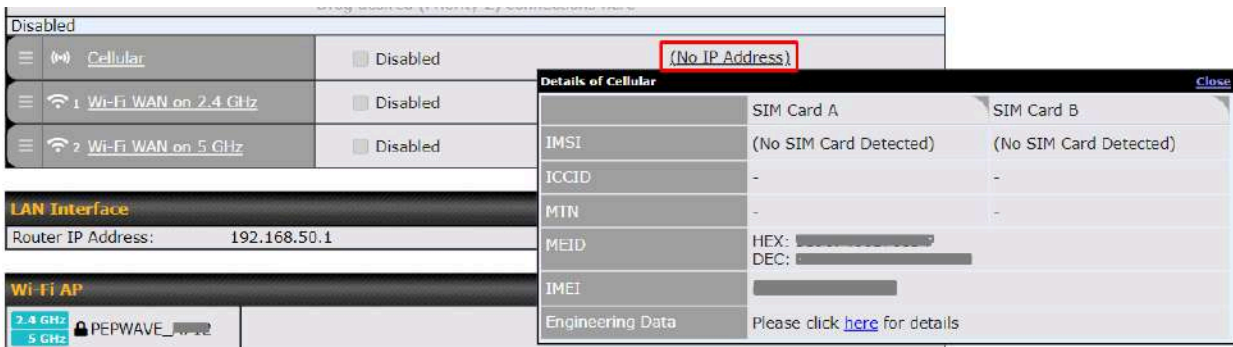
This field allows you to enter the IP address of the remote GRE.

Tunnel Local IP Address	This field allows you to enter the IP address of the local tunnel for the GRE tunnel connection.
Tunnel Remote IP Address	This field allows you to enter the IP address of the remote tunnel for the GRE tunnel connection.
Outgoing NAT IP Address	This field is to enter the NAT IP address for outgoing via GRE tunnel.
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.)</p> <p>When Use the following DNS server address(es) is selected, you can enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.</p>

8.2 Cellular WAN



To access/configure the Cellular WAN settings, click **Network > Cellular Name**. You may click the “**No IP Address**” link to view the Cellular WAN details/status.




WAN Connection Status	
IMSI	This is the International Mobile Subscriber Identity which uniquely identifies the SIM card. This is applicable to 3G modems only.
ICCID	This is a unique number assigned to a SIM card used in a cellular device.
MTN	This field is to display the mobile telephone number of the SIM card.
MEID	Some Pepwave routers support both HSPA and EV-DO. For Sprint or Verizon Wireless EV-DO users, a unique MEID identifier code (in hexadecimal format) is used by the carrier to associate the EV-DO device with the user. This information is presented in hex and decimal format.
IMEI	This is the unique ID for identifying the modem in GSM/HSPA mode.

WAN Connection Settings ?	
WAN Connection Name	<input type="text" value="Cellular"/>
Enable	<input checked="" type="checkbox"/>
Connection Priority	<input checked="" type="radio"/> Always-on (Priority 1) <input type="radio"/> Backup
Independent from Backup WANs ?	<input type="checkbox"/>
Routing Mode ?	<input checked="" type="radio"/> NAT
Management IP Address	<input type="text"/> 255.255.255.0 (/24) ▼
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>
IP Passthrough ?	<input type="checkbox"/>
Standby State ?	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Idle Disconnect	<input type="checkbox"/>
Reply to ICMP Ping ?	<input checked="" type="radio"/> Yes <input type="radio"/> No

WAN Connection Settings	
WAN Connection Name	Indicate a name you wish to give this Cellular WAN connection
Enable	Click the checkbox to toggle the on and off state of this connection.
Connection Priority	<p>This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only.</p> <p>If Always-on is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections.</p> <p>If Backup is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.</p>
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Routing Mode	<p>This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (Network Address Translation) or IP Forwarding.</p> <p>In the case if you need to choose IP Forwarding for your scenario. Click the ?</p>

	<p>button to enable IP Forwarding.</p>
Management IP Address	<p>Management IP Address is available for configuration when you click here for other DHCP settings.</p> <p>This option allows you to configure the management IP address for the DHCP WAN connection.</p>
DNS Servers	<p>Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by the DHCP server.)</p> <p>When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS server 1 and DNS server 2 fields.</p>
IP Passthrough	<p>When this IP Passthrough option is active, after the cellular WAN connection is up, the router's DHCP server will offer the connection's IP address to one LAN client. All incoming or outgoing traffic will be routed without NAT.</p> <p>Regardless the WAN connection's state, the router always binds to the LAN IP address (Default: 192.168.50.1). So when the cellular WAN is connected, the LAN client could access the router's web admin by manually configuring its IP address to the same subnet as the router's LAN IP address (e.g. 192.168.50.10).</p> <p>Note: when this option is firstly enabled, the LAN client may not be able to refresh its IP address to the cellular WAN IP address in a timely fashion. The LAN client may have to manually renew its IP address from DHCP server. After this option is enabled, the DHCP lease time will be 2 minutes. I.e. the LAN client could refresh its IP address and access the network at most one minute after the cellular WAN connection goes up</p>
Standby State	<p>This option allows you to choose whether to remain connected or disconnected when this WAN connection is no longer in the highest priority and has entered the standby state. When Remain connected is chosen, bringing up this WAN connection to active makes it immediately available for use.</p>
Idle Disconnect	<p>If this is checked, the connection will disconnect when idle after the configured Time value.</p> <p>This option is disabled by default.</p>
Reply to ICMP PING	<p>If the checkbox is unticked, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection.</p> <p>Default: ticked (Yes)</p>

Cellular Settings		
SIM Card	<input type="radio"/> Alternate between SIM A and SIM B periodically <input checked="" type="radio"/> Custom Selection <input checked="" type="checkbox"/> SIM A Priority: <input type="text" value="2"/> <input checked="" type="checkbox"/> SIM B Priority: <input type="text" value="3"/> <input checked="" type="checkbox"/> RemoteSIM Priority: <input type="text" value="4"/> <input checked="" type="checkbox"/> SpeedFusion Connect 5G/LTE Priority: <input type="text" value="1"/>	
RemoteSIM Settings	Control by FusionSIM Cloud  Scan nearby RemoteSIM server	
Failback to Preferred SIM when	<input checked="" type="checkbox"/> Device is idle Idle Timeout: <input type="text" value="3"/> <small>Time value is global. A change will affect all WAN profiles.</small> <input type="checkbox"/> Non-preferred SIM is connected for <input type="text" value="10"/> minutes	
	SIM Card A	SIM Card B
Carrier Selection	<input checked="" type="radio"/> Auto <input type="radio"/> Manual Select <input type="radio"/> Custom PLMN	<input checked="" type="radio"/> Auto <input type="radio"/> Manual Select <input type="radio"/> Custom PLMN
LTE/3G	<input type="text" value="Auto"/>	<input type="text" value="Auto"/>
Optimal Network Discovery	<input type="checkbox"/>	<input type="checkbox"/>
Band Selection	<input type="text" value="Auto"/>	<input type="text" value="Auto"/>
Data Roaming	<input type="checkbox"/>	<input type="checkbox"/>
Authentication	<input type="text" value="Auto"/>	<input type="text" value="Auto"/>
Operator Settings	<input checked="" type="radio"/> Auto <input type="radio"/> Custom	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
APN		
Username		
Password		
Confirm Password		
SIM PIN (Optional)	<input type="text"/> <input type="text"/> (Confirm)	<input type="text"/> <input type="text"/> (Confirm)
Bandwidth Allowance Monitor	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
Action	<input checked="" type="checkbox"/> Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance	<input type="checkbox"/> Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance
Start Day	On <input type="text" value="1st"/> of each month at 00:00 midnight	On <input type="text" value="1st"/> of each month at 00:00 midnight
Monthly Allowance	<input type="text"/> GB	<input type="text"/> GB

Cellular Settings

SIM Card	<p>If “Alternate between SIM A and SIM B periodically” is selected, the SIM card will be switching according to the schedule time in the SIM Cards Alternate.</p> <p>If “Custom Selection” is selected, you can designate the priority of the SIM cards (SIM A/ SIM B/ Remote SIM/ SpeedFusion Connect) and connect to.</p> <p>For routers that support the SIM Injector, you may select the “Remote SIM” to provision a SIM from a SIM Injector. Further details on the SIM Injector found is available here: https://www.peplink.com/products/sim-injector/.</p>				
Remote SIM Settings	<p>If “Use Remote SIM Only” is selected in the SIM card section, the Remote SIM Settings will be shown.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #eee; padding: 2px;">RemoteSIM Settings</td> <td style="padding: 2px;">Control by FusionSIM Cloud G</td> </tr> <tr> <td colspan="2" style="padding: 2px;">Scan nearby RemoteSIM server</td> </tr> </table> </div> <p>You may need to enable the remote SIM Host settings in the Remote SIM management, see the section 22.10 or Appendix B for more details on FusionSIM. After that, click on “Scan nearby remote SIM server” to show the serial number(s) of the connected SIM Injector(s).</p> <p>If you want to select a specific SIM, in the Cellular Settings, type “:” and then the number of the SIM slot, eg.1111-2222-3333:7.</p>	RemoteSIM Settings	Control by FusionSIM Cloud G	Scan nearby RemoteSIM server	
RemoteSIM Settings	Control by FusionSIM Cloud G				
Scan nearby RemoteSIM server					
Fallback to Preferred SIM when	<p>This option is allowing to switch to another SIM cards when the Cellular WAN reached failback timeout.</p>				
SIM Cards Alternate	<p>If “Alternate between SIM A and SIM B periodically” is selected in the SIM Card section, the SIM Cards Alternate will be shown:</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #eee; padding: 2px;">SIM Card</td> <td style="padding: 2px;"> <input checked="" type="radio"/> Alternate between SIM A and SIM B periodically <input type="radio"/> Custom Selection </td> </tr> <tr> <td style="background-color: #eee; padding: 2px;">SIM Cards Alternate</td> <td style="padding: 2px;">At <input type="text" value="00:00"/> of each month <input type="text" value="Last day"/> View Schedule</td> </tr> </table> </div> <p>You may set the schedule time for for switching between SIM A only and SIM B only.</p>	SIM Card	<input checked="" type="radio"/> Alternate between SIM A and SIM B periodically <input type="radio"/> Custom Selection	SIM Cards Alternate	At <input type="text" value="00:00"/> of each month <input type="text" value="Last day"/> View Schedule
SIM Card	<input checked="" type="radio"/> Alternate between SIM A and SIM B periodically <input type="radio"/> Custom Selection				
SIM Cards Alternate	At <input type="text" value="00:00"/> of each month <input type="text" value="Last day"/> View Schedule				
5G/LTE/3G	<p>This drop-down menu allows restricting cellular to particular band. Click the button to enable the selection of specific bands.</p>				
Optimal Network Discovery	<p>Cellular WANs by default will only handover from 3G to LTE network when there is no active data traffic, enable this option will make it run the handover procedures after fallback to 3G for a defined effective period, even this may interrupt the connectivity for a short while.</p>				
Band Selection	<p>When set to Auto, band selection allows for automatically connecting to available, supported bands (frequencies) .</p>				

	When set to Manual, you can manually select the bands (frequencies) the SIM will connect to.
Data Roaming	This checkbox enables data roaming on this particular SIM card. When data roaming is enabled this option allows you to select in which countries the SIM has a data connection. The option is configured by using MMC (country) codes. Please check your service provider's data roaming policy before proceeding.
Authentication	Choose from PAP Only or CHAP Only to use those authentication methods exclusively. Select Auto to automatically choose an authentication method.
Operator Settings	This setting allows you to configure the APN settings of your connection. If Auto is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connection, you may select Custom to enter your carrier's APN , Login , Password , and Dial Number settings manually. The correct values can be obtained from your carrier. The default and recommended setting is Auto .
APN / Login / Password / SIM PIN	When Auto is selected, the information in these fields will be filled automatically. Select Custom to customize these parameters. The parameter values are determined by and can be obtained from the ISP.
Bandwidth Allowance Monitor	Check the box Enable to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.
Action	If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If Disconnect when usage hits 100% of monthly allowance is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

Signal Threshold Settings



If signal threshold is defined, this connection will be treated as down when a weaker than threshold signal is determined.

The following values are used by the threshold scale:

	0 bars	1 bar	2 bars	3 bars	4 bars	5 bars
LTE / RSRP	-140	-128	-121	-114	-108	-98
3G / RSSI	-120	-100	-95	-90	-85	-75

To define the threshold manually using specific signal strength values, please click on the question Mark and the following field will be visible.

Signal Threshold Settings ?

LTE	RSRP: <input type="text" value="n/a"/> dBm	(Recovery: <input type="text" value="n/a"/> dBm)
	SINR: <input type="text" value="n/a"/> dB	(Recovery: <input type="text" value="n/a"/> dB)
3G	RSSI: <input type="text" value="n/a"/> dBm	(Recovery: <input type="text" value="n/a"/> dBm)

8.3 Wi-Fi WAN

Disabled

<div style="display: flex; align-items: center;"> ☰ (+) Cellular </div>	<input type="checkbox"/> Disabled (No IP Address)	
<div style="display: flex; align-items: center;"> ☰ 📶 1 Wi-Fi WAN on 2.4 GHz ↖ </div>	<input type="checkbox"/> Disabled (No IP Address)	📶
<div style="display: flex; align-items: center;"> ☰ 📶 2 Wi-Fi WAN on 5 GHz </div>	<input type="checkbox"/> Disabled (No IP Address)	📶


To access/configure the Cellular WAN settings, click **Network > Wi-Fi WAN Connection Name**.





WAN Connection Settings

WAN Connection Name	<input type="text" value="Wi-Fi WAN on 2.4 GHz"/>
Enable	<input checked="" type="checkbox"/>
Connection Priority	<input checked="" type="radio"/> Always-on (Priority 1) <input type="radio"/> Backup
Independent from Backup WANs ?	<input type="checkbox"/>
Routing Mode ?	<input checked="" type="radio"/> NAT <input type="radio"/> IP Forwarding
Standby State ?	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Reply to ICMP Ping ?	<input checked="" type="radio"/> Yes <input type="radio"/> No

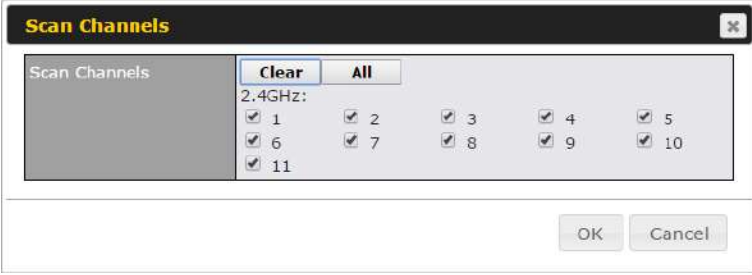

WAN Connection Settings

WAN Connection Name Enter a name to represent this Wi-Fi WAN connection.

Enable	Click the checkbox to toggle the on and off state of this connection.
Connection Priority	<p>This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only.</p> <p>If Always-on is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections.</p> <p>If Backup is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.</p>
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Routing Mode	<p>This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (Network Address Translation) or IP Forwarding.</p> <p>In the case if you need to choose IP Forwarding for your scenario. Click the  button to enable IP Forwarding.</p>
Standby State	This setting specifies the state of the WAN connection while in standby. The available options are Remain Connected and Disconnect .
Reply to ICMP PING	If this setting is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled.

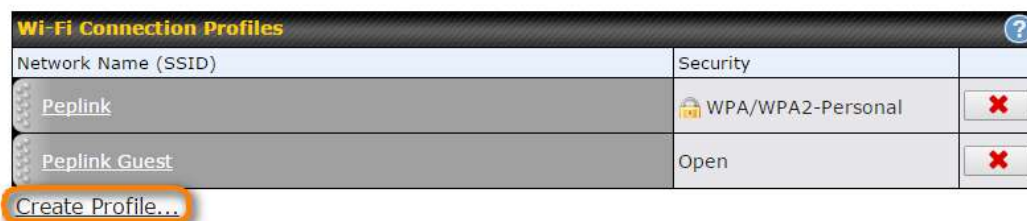
Wi-Fi WAN Settings 	
Channel Width	Auto 
Channel	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
Output Power	Max  <input type="checkbox"/> Boost
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed
Roaming	<input type="checkbox"/> Enable
Connect to Any Open Mode AP 	<input type="radio"/> Yes <input checked="" type="radio"/> No
Beacon Miss Counter	<input type="text" value="5"/>
Channel Scan Interval	<input type="text" value="50"/> ms

Wi-Fi WAN Settings	
Channel Width	Select the channel width for this Wi-Fi WAN. 20MHz will have greater support for older devices using 2.4Ghz, while 40MHz is appropriate for networks with newer devices that connect using 5Ghz

<p>Channel</p>	<p>Determine whether the channel will be automatically selected. If you select custom, the following table will appear:</p> 
<p>Output Power</p>	<p>If you are setting up a network with many Wi-Fi devices in close proximity, then you can configure the output power here. Click the “boost” button for additional power. However, with that option ticked, output power may exceed local regulatory limits.</p>
<p>Data Rate</p>	<p>Selecting Auto will enable the router to automatically determine the best data rate, while manually selecting a rate will force devices to connect using the fixed rate.</p>
<p>Roaming</p>	<p>Checking this box will enable Wi-Fi roaming. Click the  icon for additional options.</p>
<p>Connect to Any Open Mode AP</p>	<p>This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.</p>
<p>Beacon Miss Counter</p>	<p>This sets the threshold for the number of missed beacons.</p>
<p>Channel Scan Interval</p>	<p>Configure Channel Scan Interval in ms.</p>

8.3.1 Creating Wi-Fi Connection Profiles

You can manually create a profile to connect to a Wi-Fi connection. This is useful for creating a profile for connecting to hidden-SSID access points. Click **Network > Wi-Fi WAN > Create Profile...** to get started.



This will open a window similar to the one shown below

Create Wi-Fi Connection Profile
✕

Wi-Fi Connection

Network Name (SSID)	<input style="width: 90%;" type="text"/>
Security	WPA2/WPA3-Personal ▼
Shared Key	<input style="width: 90%;" type="text"/> <input checked="" type="checkbox"/> Hide Characters
Preferred BSSID	<input type="checkbox"/>
Connection Method	? DHCP ▼ <small>Click here for other DHCP settings</small>
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input style="width: 80%;" type="text"/> DNS Server 2: <input style="width: 80%;" type="text"/>

Wi-Fi Connection Profile Settings	
Network Name (SSID)	Enter a name to represent this Wi-Fi connection.
Security	This option allows you to select which security policy is used for this wireless network. Available options: <ul style="list-style-type: none"> Open WEP Enhanced Open (OWE) WPA3 -Personal WPA2/WPA3 -Personal WPA/ WPA2 – Personal WPA/ WPA2 – ENTERprise 802.1X with dynamic WEP key
Shared Key	Enter the password for the wireless network.
Preferred BSSID	Configure the BSSID. The BSSID is the MAC address of the wireless access point (WAP).
Connected Method	Choose DHCP or Static IP for the Wi-Fi WAN connection method.
DNS Servers	Configure the DNS servers that this WAN connection should use.

8.4 WAN Connection Settings (Common)

The remaining WAN-related settings are common to the WAN connection:

Physical Interface Settings	
Port Speed	<input type="text" value="Auto"/>
MTU	<input type="radio"/> Auto <input checked="" type="radio"/> Custom <input type="text" value="1440"/>
MSS	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
MAC Address Clone	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="10:56:CA:15:92:5D"/>
VLAN	<input type="checkbox"/>

Physical Interface Settings	
Speed	<p>This is the port speed of the WAN connection. It should be set to the same speed as the connected device in case of any port negotiation problems.</p> <p>When a static speed is set, you may choose whether to advertise its speed to the peer device or not. Advertise Speed is selected by default. You can choose not to advertise the port speed if the port has difficulty in negotiating with the peer device.</p> <p>Default: Auto</p>
MTU	<p>This field is for specifying the Maximum Transmission Unit value of the WAN connection. An excessive MTU value can cause file downloads stall shortly after connected. You may consult your ISP for the connection's MTU value. Default value is 1440.</p>
MSS	<p>This field is for specifying the Maximum Segment Size of the WAN connection.</p> <p>When Auto is selected, MSS will be depended on the MTU value. When Custom is selected, you may enter a value for MSS. This value will be announced to remote TCP servers for maximum data that it can receive during the establishment of TCP connections.</p> <p>Some Internet servers are unable to listen to MTU setting if ICMP is filtered by firewall between the connections.</p> <p>Normally, MSS equals to MTU minus 40. You are recommended to reduce the MSS only if changing of the MTU value cannot effectively inform some remote servers to size down data size.</p> <p>Default: Auto</p>
MAC Address Clone	<p>Some service providers (e.g. cable network) identify the client's MAC address and require client to always use the same MAC address to connect to the network. If it is the case, you may change the WAN interface's MAC address to the client PC's one by entering the PC's MAC address to this field. If you are not sure, click the Default button to restore to the default value.</p>

VLAN Check the box to assign a VLAN to the interface.

8.5 WAN Health Check

To ensure traffic is routed to healthy WAN connections only, the Pepwave router can periodically check the health of each WAN connection. The health check settings for each WAN connection can be independently configured via **Network > WAN Connection Name**

Health Check Settings											
Method	This setting specifies the health check method for the WAN connection. This value can be configured as Disabled , PING , DNS Lookup , or HTTP . The default method is DNS Lookup . For mobile Internet connections, the value of Method can be configured as Disabled or SmartCheck .										
Health Check Disabled											
<table border="1"> <tr> <td>Health Check Method</td> <td> <input type="text" value="Disabled"/> <small>Health Check disabled. Network problem cannot be detected.</small> </td> </tr> </table>		Health Check Method	<input type="text" value="Disabled"/> <small>Health Check disabled. Network problem cannot be detected.</small>								
Health Check Method	<input type="text" value="Disabled"/> <small>Health Check disabled. Network problem cannot be detected.</small>										
<p>When Disabled is chosen in the Method field, the WAN connection will always be considered as up. The connection will NOT be treated as down in the event of IP routing errors.</p>											
Health Check Method: PING											
<table border="1"> <tr> <td>Health Check Method</td> <td> <input type="text" value="PING"/> </td> </tr> <tr> <td>PING Hosts</td> <td> <table border="1"> <tr> <td>Host 1:</td> <td><input type="text"/></td> </tr> <tr> <td>Host 2:</td> <td><input type="text"/></td> </tr> <tr> <td colspan="2"> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts </td> </tr> </table> </td> </tr> </table>		Health Check Method	<input type="text" value="PING"/>	PING Hosts	<table border="1"> <tr> <td>Host 1:</td> <td><input type="text"/></td> </tr> <tr> <td>Host 2:</td> <td><input type="text"/></td> </tr> <tr> <td colspan="2"> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts </td> </tr> </table>	Host 1:	<input type="text"/>	Host 2:	<input type="text"/>	<input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts	
Health Check Method	<input type="text" value="PING"/>										
PING Hosts	<table border="1"> <tr> <td>Host 1:</td> <td><input type="text"/></td> </tr> <tr> <td>Host 2:</td> <td><input type="text"/></td> </tr> <tr> <td colspan="2"> <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts </td> </tr> </table>	Host 1:	<input type="text"/>	Host 2:	<input type="text"/>	<input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts					
Host 1:	<input type="text"/>										
Host 2:	<input type="text"/>										
<input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts											
<p>ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.</p>											
PING Hosts	This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If Use first two DNS servers as Ping Hosts is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.										
Health Check Method: DNS Lookup											

Health Check Method	? DNS Lookup
Health Check DNS Servers	Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers

DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.

Health Check DNS Servers

This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS lookup.

If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional.

If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers.

Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP

HTTP connections will be issued to test connectivity with configurable URLs and strings to match.

Health Check Method	? HTTP
URL 1	? http:// <input type="text"/> Matching String: <input type="checkbox"/>
URL 2	? http:// <input type="text"/> Matching String: <input type="checkbox"/>

URL 1





WAN Settings>WAN Edit>Health Check Settings>URL1

The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.

URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2


If **URL2** is also provided, a health check will pass if either one of the tests passed.

Timeout		10 ▾ second(s)
Health Check Interval		5 ▾ second(s)
Health Check Retries		3 ▾
Recovery Retries		3 ▾

Other Health Check Settings	
Timeout	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is 5 seconds .
Health Check Interval	This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is 5 seconds .
Health Check Retries	This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Pepwave router will treat the corresponding WAN connection as down. Default health retries is set to 3 . Using the default Health Retries setting of 3 , the corresponding WAN connection will be treated as down after three consecutive timeouts.
Recovery Retries	This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Pepwave router treats a previously down WAN connection as up again. By default, Recover Retries is set to 3 . Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.

Automatic Public DNS Server Check on DNS Test Failure

When the health check method is set to **DNS Lookup** and health checks fail, the Pepwave router will automatically perform DNS lookups on public DNS servers. If the tests are successful, the WAN may not be down, but rather the target DNS server malfunctioned. You will see the following warning message on the main page:

 **Failed to receive DNS response from the health-check DNS servers for WAN connection 3. But public DNS server lookup test via the WAN passed. So please check the DNS server settings.**

8.6 Bandwidth Allowance Monitoring

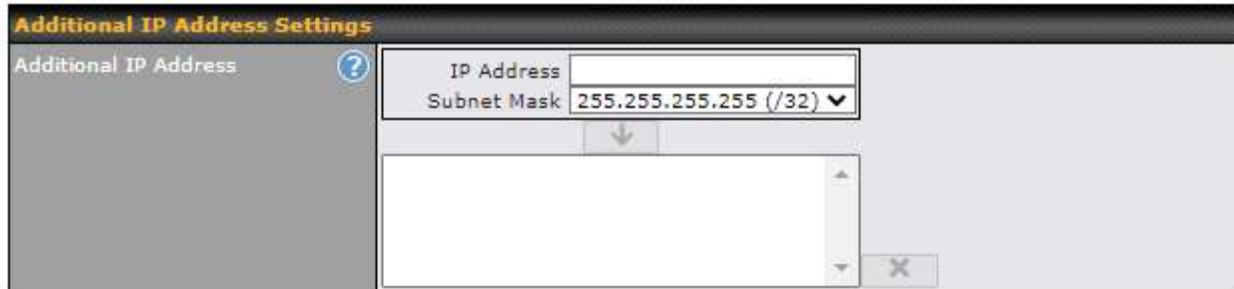
Bandwidth Allowance Monitor	
Bandwidth Allowance Monitor ?	<input checked="" type="checkbox"/> Enable
Action ?	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance
Start Day ?	On <input type="text" value="1st"/> of each month at 00:00 midnight
Monthly Allowance ?	<input type="text"/> GB

Bandwidth Allowance Monitor	
Action	<p>If Email Notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance.</p> <p>If Disconnect when usage hits 100% of monthly allowance is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.</p>
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

Disclaimer

Due to different network protocol overheads and conversions, the amount of data reported by this Peplink device is not representative of actual billable data usage as metered by your network provider. Peplink disclaims any obligation or responsibility for any events arising from the use of the numbers shown here.

8.7 Additional Public IP address



Additional Public IP Settings

IP Address List represents the list of fixed Internet IP addresses assigned by the ISP in the event that more than one Internet IP address is assigned to this WAN connection. Enter the fixed Internet IP addresses and the corresponding subnet mask, and then click the **Down Arrow** button to populate IP address entries to the **IP Address List**.

8.8 Dynamic DNS Settings

Pepwave routers are capable of registering the domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a host name. With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address from the external, even if its IP address is dynamic. You must register for an account from the listed dynamic DNS service providers before enabling this option.

If the WAN connection's IP address is a reserved private IP address (i.e., behind a NAT router), the public IP of each WAN will be automatically reported to the DNS service provider.

Either upon a change in IP addresses or every 23 days without link reconnection, the Pepwave router will connect to the dynamic DNS service provider to perform an IP address update within the provider's records.

The settings for dynamic DNS service provider(s) and the association of hostname(s) are configured via **Network > WAN > Details > Dynamic DNS Service Provider/Dynamic DNS Settings**.

Dynamic DNS Service Provider	changeip.com ▾
User ID	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Hosts	<input type="text"/>

Dynamic DNS Settings

Dynamic DNS

This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:

- Disabled
- changeip.com
- dyndns.org
- no-ip.org
- DNS-O-Matic
- Others...

Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.

Select **Disabled** to disable this feature.

User ID/ Username / Email

This setting specifies the registered user name for the dynamic DNS service.

Password

This setting specifies the password for the dynamic DNS service.

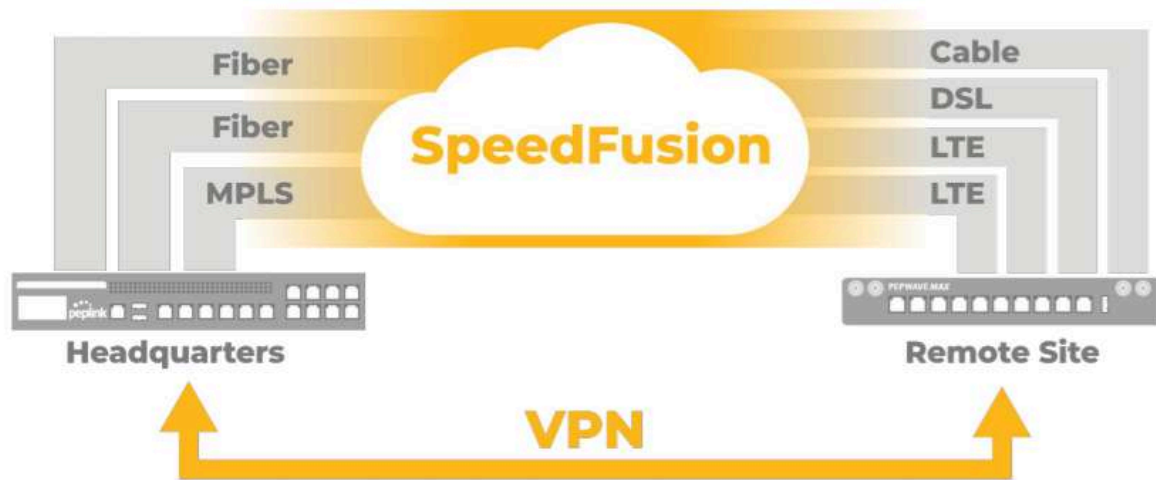
Hosts

This field allows you to specify a list of host names or domains to be associated with the public Internet IP address of the WAN connection. If you need to enter more than one host, use a carriage return to separate them.

Important Note

In order to use dynamic DNS services, appropriate host name registration(s) and a valid account with a supported dynamic DNS service provider are required. A dynamic DNS update is performed whenever a WAN's IP address changes (e.g., the IP is changed after a DHCP IP refresh, reconnection, etc.). Due to dynamic DNS service providers' policy, a dynamic DNS host will automatically expire if the host record has not been updated for a long time. Therefore the Pepwave router performs an update every 23 days, even if a WAN's IP address has not changed.

9 SpeedFusion VPN



Pepwave bandwidth bonding SpeedFusion™ is our patented technology that enables our SD-WAN routers to bond multiple Internet connections to increase site-to-site bandwidth and reliability. SpeedFusion functionality securely connects your Pepwave router to another Pepwave or Peplink device (Peplink Balance 210/310/380/580/710/1350 only). Data, voice, or video communications between these locations are kept confidential across the public Internet.

Bandwidth bonding SpeedFusion™ is specifically designed for multi-WAN environments. In case of failures and network congestion at one or more WANs, other WANs can be used to continue carrying the network traffic.

Different models of our SD-WAN routers have different numbers of site-to-site connections allowed. End-users who need to have more site-to-site connections can purchase a SpeedFusion license to increase the number of site-to-site connections allowed.

Pepwave routers can aggregate all WAN connections' bandwidth for routing SpeedFusion™ traffic. Unless all the WAN connections of one site are down, Pepwave routers can keep the VPN up and running.

VPN bandwidth bonding is supported in Firmware 5.1 or above. All available bandwidth will be utilized to establish the VPN tunnel, and all traffic will be load balanced at packet level across all links. VPN bandwidth bonding is enabled by default.

9.1 SpeedFusion VPN

To configure SpeedFusion VPN, navigate to **Advanced > SpeedFusion VPN**.

The local LAN subnet and subnets behind the LAN (defined under **Static Route** on the LAN settings page) will be advertised to the VPN. All VPN members (branch offices and headquarters) will be able to route to local subnets.



Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other.

All data can be routed over the VPN using the 256-bit AES encryption standard. To configure, navigate to **Advanced > SpeedFusion VPN** and click the **New Profile** button to create a new VPN profile (you may have to first save the displayed default profile in order to access the **New Profile** button). Each profile specifies the settings for making VPN connection with one remote Pepwave or Peplink device. Note that available settings vary by model.

A list of defined SpeedFusion connection profiles and a **Link Failure Detection Time** option will be shown. Click the **New Profile** button to create a new VPN connection profile for making a VPN connection to a remote Pepwave or Peplink device via the available WAN connections. Each profile is for making a VPN connection with one remote Pepwave or Peplink Device.

SpeedFusion VPN Profile					
Name	<input type="text"/>				
Enable	<input checked="" type="checkbox"/>				
Encryption	<input checked="" type="radio"/> 256-bit AES <input type="radio"/> OFF				
Authentication	<input checked="" type="radio"/> Remote ID / Pre-shared Key				
Remote ID / Pre-shared Key	<table border="1"> <tr> <td>Remote ID</td> <td>Pre-shared Key</td> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </table>	Remote ID	Pre-shared Key	<input type="text"/>	<input type="text"/>
Remote ID	Pre-shared Key				
<input type="text"/>	<input type="text"/>				
NAT Mode	<input type="checkbox"/>				
Remote IP Address / Host Names (Optional)	<input type="text"/> <small>If this field is empty, this field on the remote unit must be filled</small>				
Cost	<input type="text" value="10"/>				
Data Port	<input checked="" type="radio"/> Auto <input type="radio"/> Custom <input type="text"/>				
Bandwidth Limit	<input type="checkbox"/>				
WAN Smoothing	<input type="text" value="Off"/>				
Forward Error Correction	<input type="text" value="Off"/>				
Receive Buffer	<input type="text" value="0"/> ms				
Packet Fragmentation	<input checked="" type="radio"/> Always <input type="radio"/> Use DF Flag				
Use IP ToS	<input type="checkbox"/>				
Latency Difference Cutoff	<input type="text" value="500"/> ms				

SpeedFusion VPN Profile Settings	
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ().
Enable	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with 256-bit AES . If Off is selected on both sides of a VPN connection, no encryption will be applied.
Authentication	Select from By Remote ID Only , Preshared Key , or X.509 to specify the method the Pepwave MAX will use to authenticate peers. When selecting By Remote ID Only , be sure to enter a unique peer ID number in the Remote ID field.
Remote ID / Pre-shared Key	This optional field becomes available when Remote ID / Pre-shared Key is selected as the Pepwave router's VPN Authentication method, as explained above. Pre-shared Key defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored.

	<p>Enter Remote IDs either by typing out each Remote ID and Pre-shared Key, or by pasting a CSV. If you wish to paste a CSV, click the  icon next to the “Remote ID / Preshared Key” setting.</p>
Remote ID/Remote Certificate	<p>These optional fields become available when X.509 is selected as the Pepwave MAX’s VPN authentication method, as explained above. To authenticate VPN connections using X.509 certificates, copy and paste certificate details into these fields. To get more information on a listed X.509 certificate, click the Show Details link below the field.</p>
Allow Shared Remote ID	<p>When this option is enabled, the router will allow multiple peers to run using the same remote ID.</p>
NAT Mode	<p>Check this box to allow the local DHCP server to assign an IP address to the remote peer. When NAT Mode is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.</p>
Remote IP Address / Host Names (Optional)	<p>If NAT Mode is not enabled, you can enter a remote peer’s WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted.</p> <p>This field is optional. With this field filled, the Pepwave MAX will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Pepwave MAX will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.</p>
Cost	<p>Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10</p>
Data Port	<p>This field is used to specify a UDP port number for transporting outgoing VPN data. If Default is selected, UDP port 4500 will be used. Port 32015 will be used if the remote unit uses Firmware prior to version 5.4 or if port 4500 is unavailable. If Custom is selected, enter an outgoing port number from 1 to 65535.</p> <p>Click the  icon to configure data stream using TCP protocol [EXPERIMENTAL].In the case TCP protocol is used, the exposed TCP session option can be authorised to work with TCP accelerated WAN link.</p>
Bandwidth Limit	<p>Define maximum download and upload speed to each individual peer. This functionality requires the peer to use SpeedFusion VPN version 4.0.0 or above.</p>
WAN Smoothing	<p>While using SpeedFusion VPN, utilize multiple WAN links to reduce the impact of packet loss and get the lowest possible latency at the expense of extra bandwidth consumption. This is suitable for streaming applications where the average bitrate requirement is much lower than the WAN’s available bandwidth.</p>

	<p>Off - Disable WAN Smoothing.</p> <p>Normal - The total bandwidth consumption will be at most 2x of the original data traffic.</p> <p>Medium - The total bandwidth consumption will be at most 3x of the original data traffic.</p> <p>High - The total bandwidth consumption depends on the number of connected active tunnels.</p>
Forward Error Correction	<p>Forward Error Correction (FEC) can help to recover packet loss by using extra bandwidth to send redundant data packets. Higher FEC level will recover packets on a higher loss rate link.</p> <p>The expected overhead of Low is 13.3% and High is 26.7%.</p> <p>Require peer using SpeedFusion VPN version 8.0.0 and above.</p>
Receive Buffer	<p>Receive Buffer can help to reduce out-of-order packets and jitter, but will introduce extra latency to the tunnel. Default is 0 ms, which disables the buffer, and maximum buffer size is 2000 ms.</p>
Packet Fragmentation	<p>If the packet size is larger than the tunnel's MTU, it will be fragmented inside the tunnel in order to pass through.</p> <p>Select Always to fragment any packets that are too large to send, or Use DF Flag to only fragment packets with Don't Fragment bit cleared. This can be useful if your application does Path MTU Discovery, usually sending large packets with DF bit set, if allowing them to go through by fragmentation, the MTU will not be detected correctly.</p>
Use IP ToS^A	<p>Checking this button enables the use of IP ToS header field.</p>
Latency Difference Cutoff^A	<p>Traffic will be stopped for links that exceed the specified millisecond value with respect to the lowest latency link. (e.g. Lowest latency is 100ms, a value of 500ms means links with latency 600ms or more will not be used)</p>

^A - Advanced feature, please click the  button on the top right-hand corner to activate.

To enable Layer 2 Bridging between SpeedFusion VPN profiles, navigate to **Network > LAN > Basic Settings > *LAN Profile Name*** and refer to instructions in section 9.1



Traffic Distribution	
Policy	<input type="text" value="Dynamic Weighted Bonding"/>
Congestion Latency Level	<input type="text" value="Default"/>
Ignore Packet Loss Event	<input type="checkbox"/>
Disable Bufferbloat Handling	<input type="checkbox"/>
Disable TCP ACK Optimization	<input type="checkbox"/>
Packet Jitter Buffer	<input type="text" value="150"/> ms

Traffic Distribution	
Policy	<p>This option allows you to select the desired out-bound traffic distribution policy:</p> <ul style="list-style-type: none"> • Bonding - Aggregate multiple WAN-to-WAN links into a single higher throughput tunnel. • Dynamic Weighted Bonding - Aggregates WAN-to-WAN links with similar latencies. <p>By default, Bonding is selected as a traffic distribution policy.</p>
Congestion Latency Level	<p>For most WANs, especially on cellular networks, the latency will increase when the link becomes more congested.</p> <p>Setting the Congestion Latency Level to Low will treat the link as congested more aggressively.</p> <p>Setting it to High will allow the latency to increase more before treating it as congested.</p>
Ignore Packet Loss Event	<p>By default, when there is packet loss, it is considered as a congestion event. If this is not the case, select this option to ignore the packet loss event.</p>
Disable Bufferbloat Handling	<p>Bufferbloat is a phenomenon on the WAN side when it is congested. The latency can become very high due to buffering on the uplink. By default, the Dynamic Weighted Bonding policy will try its best to mitigate bufferbloat by reducing TCP throughput when the WAN is congested. However, as a side effect, the tunnel might not achieve maximum bandwidth.</p> <p>Selecting this option will disable the bufferbloat handling mentioned above.</p>
Disable TCP ACK Optimization	<p>By default, TCP ACK will be forwarded to remote peers as fast as possible. This will consume more bandwidth, but may help to improve TCP performance as well.</p> <p>Selecting this option will disable the TCP ACK optimization mentioned above.</p>
Packet Jitter Buffer	<p>The default jitter buffer is 150ms, and can be modified from 0ms to 500ms. The jitter buffer may increase the tunnel latency. If you want to keep the latency as low as possible, you can set it to 0ms to disable the buffer.</p> <p>Note: If the Receive Buffer is set, the Packet Jitter Buffer will be automatically disabled.</p>

WAN Connection Priority ?					
	Priority	Direction	Connect to Remote	Cut-off latency (ms)	Suspension Time after Packet Loss (ms)
1. WAN 1	1 (Highest) ▼	Up/Down ▼	All ▼	<input type="text"/>	<input type="text"/>
2. WAN 2	1 (Highest) ▼	Up/Down ▼	All ▼	<input type="text"/>	<input type="text"/>
3. Wi-Fi WAN	1 (Highest) ▼	Up/Down ▼	All ▼	<input type="text"/>	<input type="text"/>
4. Cellular 1	1 (Highest) ▼	Up/Down ▼	All ▼	<input type="text"/>	<input type="text"/>
5. Cellular 2	1 (Highest) ▼	Up/Down ▼	All ▼	<input type="text"/>	<input type="text"/>
6. USB	1 (Highest) ▼	Up/Down ▼	All ▼	<input type="text"/>	<input type="text"/>

WAN Connection Priority

WAN Connection Priority

If your device supports it, you can specify the priority of WAN connections to be used for making VPN connections. WAN connections set to **OFF** will never be used. Only available WAN connections with the highest priority will be used.

To enable asymmetric connections, connection mapping to remote WANs, cut-off latency, and packet loss suspension time, click the ? button.

Send All Traffic To

No SpeedFusion VPN profile selected ?

Send All Traffic To

This feature allows you to redirect all traffic to a specified SpeedFusion VPN connection. Click the ? button to select your connection and the following menu will appear:

Send All Traffic

Send All Traffic To ?

Balance 2942-1257-1241 ▼

DNS Server

Backup Site Balance-4810-1825-068E-4810 ▼

DNS Server

You could also specify a DNS server to resolve incoming DNS requests. Click the checkbox next to **Backup Site** to designate a backup SpeedFusion profile that will take over, should the main SpeedFusion VPN connection fail.

Outbound Policy/SpeedFusion VPN Outbound Custom Rules


Some models allow you to set outbound policy and custom outbound rules from **Advanced>SpeedFusion VPN**. See **Section 14** for more information on outbound policy settings.

The screenshot shows two configuration sections. The first, 'Outbound Policy', has a dropdown menu set to 'According to custom rules' and a red edit icon. The second, 'PepVPN Outbound Custom Rules', is a table with columns for Service, Algorithm, Source, Destination, and Protocol. The Protocol column contains '(Auto)'. Below the table is an 'Add Rule' button.

SpeedFusion VPN Local ID

The screenshot shows a configuration field for 'Local ID' with a question mark icon on the left and a red edit icon on the right. The text 'MAX-BR1-A712' is entered in the field.

SpeedFusion VPN Local ID

The local ID is a text string to identify this local unit when establishing a VPN connection. When creating a profile on a remote unit, this local ID must be entered in the remote unit's **Remote ID** field. Click the  icon to edit **Local ID**.

SpeedFusion VPN Settings

The screenshot shows the 'SpeedFusion VPN Settings' configuration page. It includes a 'Handshake Port' section with radio buttons for 'Default' (selected) and 'Custom' (with an input field). Below is a 'Link Failure Detection Time' section with radio buttons for 'Recommended (Approx. 15 secs)' (selected), 'Fast (Approx. 6 secs)', 'Faster (Approx. 2 secs)', and 'Extreme (Under 1 sec)'. A note below the radio buttons states: 'Shorter detection time incurs more health checks and higher bandwidth overhead'. A 'Save' button is at the bottom.

SpeedFusion VPN Settings

Handshake Port^A To designate a custom handshake port (TCP), click the **custom** radio button and enter the port number you wish to designate.

Link Failure Detection Time The bonded VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the remote unit to detect any failure. The more frequently checks are sent, the shorter the detection time, although more bandwidth will be consumed.


When **Recommended** (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds.

When **Fast** is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds.

When **Faster** is selected, a health check packet is sent every second, and the

expected detection time is two seconds.

When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

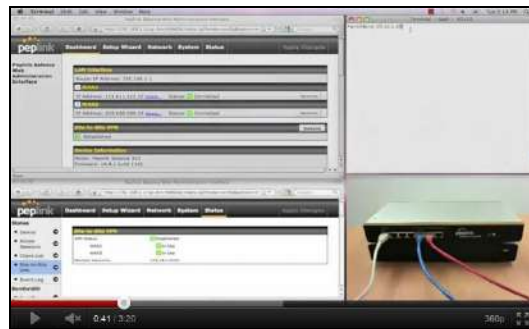
^A - Advanced feature, please click the  button on the top right-hand corner to activate.

Important Note

Peplink proprietary SpeedFusion™ uses TCP port 32015 and UDP port 4500 for establishing VPN connections. If you have a firewall in front of your Pepwave devices, you will need to add firewall rules for these ports and protocols to allow inbound and outbound traffic to pass through the firewall.

Tip

Want to know more about VPN sub-second session failover? Visit our YouTube Channel for a video tutorial!



<http://youtu.be/TLQgdpPSY88>

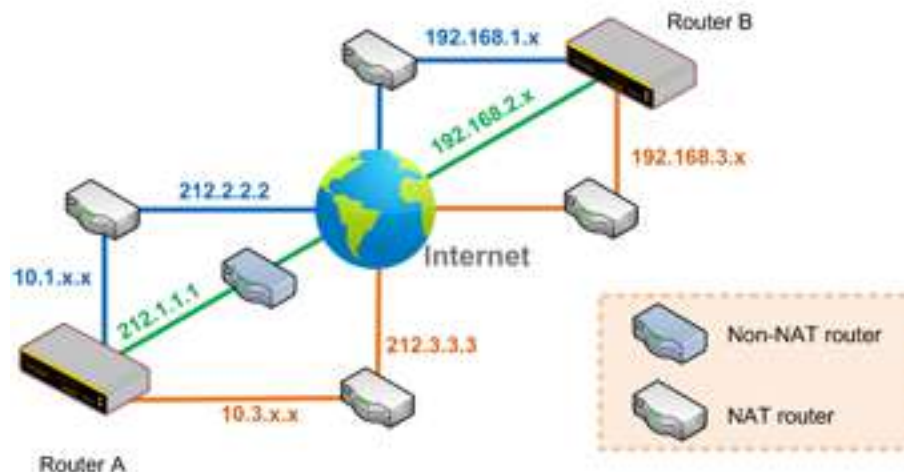
9.2 The Pepwave Router Behind a NAT Router

Pepwave routers support establishing SpeedFusion™ over WAN connections which are behind a NAT (network address translation) router.

To enable a WAN connection behind a NAT router to accept VPN connections, you can configure the NAT router in front of the WAN connection to inbound port-forward TCP port 32015 to the Pepwave router.

If one or more WAN connections on Unit A can accept VPN connections (by means of port forwarding or not), while none of the WAN connections on the peer Unit B can do so, you should enter all of Unit A's public IP addresses or hostnames into Unit B's **Remote IP Addresses / Host Names** field. Leave the field in Unit A blank. With this setting, a SpeedFusion™ connection can be set up and all WAN connections on both sides will be utilized.

See the following diagram for an example of this setup in use:



One of the WANs connected to Router A is non-NAT'd (212.1.1.1). The rest of the WANs connected to Router A and all WANs connected to Router B are NAT'd. In this case, the **Peer IP Addresses / Host Names** field for Router B should be filled with all of Router A's hostnames or public IP addresses (i.e., 212.1.1.1, 212.2.2.2, and 212.3.3.3), and the field in Router A can be left blank. The two NAT routers on WAN1 and WAN3 connected to Router A should inbound port-forward TCP port 32015 to Router A so that all WANs will be utilized in establishing the VPN.

9.3 SpeedFusion VPN Status

SpeedFusion VPN status is shown in the Dashboard. The connection status of each connection profile is shown as below.

SpeedFusion VPN		Status
To MK2	 Established	

After clicking the **Status** button at the top right corner of the SpeedFusion™ table, you will be forwarded to **Status > SpeedFusion VPN**, where you can view subnet and WAN connection information for each VPN peer.

IP Subnets Must Be Unique Among VPN Peers

The entire interconnected SpeedFusion™ network is a single non-NAT IP network. Avoid duplicating subnets in your sites to prevent connectivity problems when accessing those subnets.

10 IPsec VPN

IPsec VPN functionality securely connects one or more branch offices to your company's main headquarters or to other branches. Data, voice, and video communications between these locations are kept safe and confidential across the public Internet.

IPsec VPN on Pepwave routers is specially designed for multi-WAN environments. For instance, if a user sets up multiple IPsec profiles for a multi-WAN environment and WAN1 is connected and healthy, IPsec traffic will go through this link. However, should unforeseen problems (e.g., unplugged cables or ISP problems) cause WAN1 to go down, our IPsec implementation will make use of WAN2 and WAN3 for failover.

10.1 IPsec VPN Settings

Many Pepwave products can make multiple IPsec VPN connections with Peplink, Pepwave, Cisco, and Juniper routers. Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other. All data can be routed over the VPN with a selection of encryption standards, such as 3DES, AES-128, and AES-256. To configure IPsec VPN on Pepwave devices that support it, navigate to **Advanced>IPsec VPN**.



Pepwave MAX IPsec only supports network-to-network connection with Cisco, Juniper or Pepwave MAX devices.

Click the **New Profile** button to create new IPsec VPN profiles that make VPN connections to remote Pepwave, Cisco, or Juniper routers via available WAN connections. To edit any of the profiles, click on its associated connection name in the leftmost column.

IPsec VPN Profile			
Name	<input type="text"/>		
Active	<input checked="" type="checkbox"/>		
IKE Version	<input checked="" type="radio"/> IKEv1 <input type="radio"/> IKEv2		
Connect Upon Disconnection of	<input checked="" type="checkbox"/>	WAN 1	
Remote Gateway IP Address / Host Name	<input type="text"/>		
IPsec Type	<input checked="" type="radio"/> Policy-based <input type="radio"/> Route-based		
Local Networks	<input checked="" type="checkbox"/>	192.168.50.0/24	
	<input type="checkbox"/>	<input type="text"/>	
Remote Networks	Network	Subnet Mask	
	<input type="text"/>	255.255.255.0 (/24)	<input type="button" value="+"/>
Authentication	<input checked="" type="radio"/> Preshared Key <input type="radio"/> X.509 Certificate		
Mode	<input checked="" type="radio"/> Main Mode (All WANs need to have Static IP) <input type="radio"/> Aggressive Mode		
Force UDP Encapsulation	<input type="checkbox"/>		
Preshared Key	<input type="text"/>		
	<input checked="" type="checkbox"/>	Hide Characters	
Local ID	<input type="text"/>		
Remote ID	<input type="text"/>		
Phase 1 (IKEv1) Proposal	1	AES-CBC-256 & SHA1	▼
	2	-----	▼
Phase 1 DH Group	1	Group 2	▼
	2	-----	▼
Phase 1 SA Lifetime	<input type="text" value="3600"/>	seconds	
Phase 2 (ESP) Proposal	1	AES-CBC-256 & SHA1	▼
	2	-----	▼
Phase 2 PFS Group	None ▼		
Phase 2 SA Lifetime	<input type="text" value="28800"/>	seconds	

IPsec VPN Profile Settings	
Name	This field is for specifying a local name to represent this connection profile.
Active	When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it will be disabled.
IKE Version	Two versions of the IKE standards are available: <ul style="list-style-type: none"> • IKEv1 • IKEv2

Connect Upon Disconnection of	Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected.
Remote Gateway IP Address / Host Name	Enter the remote peer's public IP address. For Aggressive Mode , this is optional.
IPsec Type	<p>Policy-based - (default) All the matched traffic as defined in Local Networks and Remote Networks will be routed to this IPsec connection, this cannot be overridden by other routing methods.</p> <p>Route-based - Outbound Policy rule is required to route traffic to this tunnel and comes with more flexibility to control how to route traffic compared to Policy-based. If you want to modify the traffic selector instead of using the default (0.0.0.0/0).</p> <p>Note: This option is available for certain following models only:</p> <ul style="list-style-type: none"> • MAX: BR1 ENT, Transit, 700 HW3 or above, HD2 HW5 or above, HD4
Local Networks	<p>Enter the local LAN subnets here. If you have defined static routes, they will be shown here.</p> <p>Using NAT, you can map a specific local network / IP address to another, and the packets received by remote gateway will appear to be coming from the mapped network / IP address. This allow you to establish IPsec connection to a remote site that has one or more subnets overlapped with local site.</p> <p>Two types of NAT policies can be defined:</p> <p>One-to-One NAT policy: if the defined subnet in Local Network and NAT Network has the same size, for example, policy "192.168.50.0/24 > 172.16.1.0/24" will translate the local IP address 192.168.50.10 to 172.16.1.10 and 192.168.50.20 to 172.16.1.20. This is a bidirectional mapping which means clients in remote site can initiate connection to the local clients using the mapped address too.</p> <p>Many-to-One NAT policy: if the defined NAT Network on the right hand side is an IP address (or having a network prefix /32), for example, policy "192.168.1.0/24 > 172.168.50.1/32" will translate all clients in 192.168.1.0/24 network to 172.168.50.1. This is a unidirectional mapping which means clients in remote site will not be able to initiate connection to the local clients.</p>
Remote Networks	Enter the LAN and subnets that are located at the remote site here.
Authentication	To access your VPN, clients will need to authenticate by your choice of methods. Choose between the Preshared Key and X.509 Certificate methods of

	authentication.
Mode	Choose Main Mode if both IPsec peers use static IP addresses. Choose Aggressive Mode if one of the IPsec peers uses dynamic IP addresses.
Force UDP Encapsulation	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.
Pre-shared Key	This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match.
Remote Certificate (pem encoded)	Available only when X.509 Certificate is chosen as the Authentication method, this field allows you to paste a valid X.509 certificate.
Local ID	In Main Mode , this field can be left blank. In Aggressive Mode , if Remote Gateway IP Address is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Remote ID	In Main Mode , this field can be left blank. In Aggressive Mode , if Remote Gateway IP Address is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Phase 1 (IKE) Proposal	In Main Mode , this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In Aggressive Mode , only one selection is permitted.
Phase 1 DH Group	This is the Diffie-Hellman group used within IKE. This allows two parties to establish a shared secret over an insecure communications channel. The larger the group number, the higher the security. Group 2: 1024-bit is the default value. Group 5: 1536-bit is the alternative option.
Phase 1 SA Lifetime	This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at 3600 seconds.
Phase 2 (ESP) Proposal	In Main Mode , this allows setting up to six encryption standards, in descending order of priority, to be used for the IP data that is being transferred. In Aggressive Mode , only one selection is permitted.
Phase 2 PFS Group	Perfect forward secrecy (PFS) ensures that if a key was compromised, the attacker will be able to access only the data protected by that key. None - Do not request for PFS when initiating connection. However, since there is no valid reason to refuse PFS, the system will allow the connection to use PFS if requested by the remote peer. This is the default value. Group 2: 1024-bit Diffie-Hellman group. The larger the group number, the higher the security. Group 5: 1536-bit is the third option.

Phase 2 SA Lifetime This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at **28800** seconds.

WAN Connection Priority	
Priority	WAN Selection
1	WAN 1
2	-----

WAN Connection Priority

WAN Connection Select the appropriate WAN connection from the drop-down menu.

10.2 GRE Tunnel

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. A GRE tunnel is similar to IPSec or SpeedFusion VPN.

To configure a GRE Tunnel, navigate to **Advanced > GRE Tunnel**.

GRE Tunnel Profiles	Remote Networks
No GRE profile defined	
New Profile	

Click the **New Profile** button to create new GRE tunnel profiles that establish tunnel connections to remote tunnel endpoints via available WAN connections. To edit the profiles, click on its associated connection name in the leftmost column.

GRE Tunnel Profile ✕

Name	<input type="text"/>		
Active	<input checked="" type="checkbox"/>		
Remote GRE IP Address	<input type="text"/>		
Tunnel Local IP Address	<input type="text"/>		
Tunnel Remote IP Address	<input type="text"/>		
Tunnel Subnet Mask	<input checked="" type="radio"/> Auto <input type="radio"/> <input type="text" value="255.255.255.0 (/24)"/>		
Connection	WAN ▼		
Remote Networks	Network	Subnet Mask	
	<input type="text"/>	<input type="text" value="255.255.255.0 (/24)"/>	<input type="button" value="+"/>

GRE Tunnel Profile Settings

Name	This field is for specifying a name to represent this GRE Tunnel connection profile.
Active	When this box is checked, this GRE Tunnel connection profile will be enabled. Otherwise, it will be disabled.
Remote GRE IP Address	This field is for entering the remote GRE's IP address
Tunnel Local IP Address	This field is for specifying the tunnel source IP address.
Tunnel Remote IP Address	This field is for specifying the tunnel destination IP address
Tunnel Subnet Mask	This field is to select the subnet mask that is to be used for the GRE tunnel.
Connection	Select the appropriate WAN connection from the drop-down menu.
Remote Networks	Input the LAN and subnets that are located at the remote site here.

11 OpenVPN

OpenVPN is a site to site VPN mode that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.

To configure a OpenVPN, navigate to **Advanced > OpenVPN** and click the **New Profile**.

OpenVPN Profile Settings	
Name	This field is for specifying a name to represent this OpenVPN profile.
Active	When this box is checked, this OpenVPN connection profile will be enabled. Otherwise, it will be disabled.
OpenVPN Profile	Upload the OpenVPN configuration (.ovpn) file from your service provider.
Login Credential (Optional)	This option is an optional for you to enter the username and password to login for the OpenVPN connection if the profile need to login.
Connection	Select the appropriate WAN connection from the drop-down menu.

12 Outbound Policy

Pepwave routers can flexibly manage and load balance outbound traffic among WAN connections.

Important Note

Outbound policy is applied only when more than one WAN connection is active.

The settings for managing and load balancing outbound traffic are located at **Advanced > Outbound Policy**.

Service	Algorithm	Source	Destination	Protocol / Port	
SpeedFusion VPN / OSPF / BGP / RIPv2 Routes					
☰ HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				
Add Rule					

Expert Mode	
Enabled	✎

12.1 Adding Rules for Outbound Policy

The menu underneath enables you to define Outbound policy rules:

Service	Algorithm	Source	Destination	Protocol / Port	
SpeedFusion VPN / OSPF / BGP / RIPv2 Routes					
☰ HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				
Add Rule					

The bottom-most rule is **Default**. Edit this rule to change the device's default manner of controlling outbound traffic for all connections that do not match any of the rules above it. Under the **Service** heading, click **Default** to change these settings.

To rearrange the priority of outbound rules, drag and drop them into the desired sequence.

Edit Default Custom Rule
✕

Default Rule ?	<input checked="" type="radio"/> Custom <input type="radio"/> Auto
Algorithm ?	Weighted Balance ▼
Load Distribution Weight ?	<div style="margin-bottom: 5px;">WAN 1 10 ●</div> <div style="margin-bottom: 5px;">WAN 2 10 ●</div> <div style="margin-bottom: 5px;">WAN 3 10 ●</div> <div style="margin-bottom: 5px;">WAN 4 10 ●</div> <div style="margin-bottom: 5px;">WAN 5 10 ●</div> <div style="margin-bottom: 5px;">Mobile Internet 10 ●</div>
When No Connections are Available ?	<div style="border: 1px solid #ccc; padding: 2px;"> Drop the Traffic ▼ Drop the Traffic Use Any Available Connections </div>

By default, **Auto** is selected as the **Default Rule**. You can select **Custom** to change the algorithm to be used. Please refer to the upcoming sections for the details on the available algorithms.

To create a custom rule, click **Add Rule** at the bottom of the table.

Add a New Custom Rule
✕

Service Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Always on ▾
Source	Any ▾
Destination	<input type="text" value="IP Network"/> ▾ <input type="text" value="Mask: 255.255.255.0 (/24)"/> ▾
Protocol	Any ▾ ◀ :: Protocol Selection :: ▾
Algorithm	Weighted Balance ▾
Load Distribution Weight	<div style="display: flex; flex-direction: column; gap: 5px;"> <div>WAN 1 10 <input type="range" value="10"/></div> <div>WAN 2 10 <input type="range" value="10"/></div> <div>WAN 3 10 <input type="range" value="10"/></div> <div>WAN 4 10 <input type="range" value="10"/></div> <div>WAN 5 10 <input type="range" value="10"/></div> <div>Mobile Internet 10 <input type="range" value="10"/></div> </div>
When No Connections are Available	Drop the Traffic ▾

New Custom Rule Settings

Service Name	This setting specifies the name of the outbound traffic rule.														
Enable	<p>This setting specifies whether the outbound traffic rule takes effect. When Enable is checked, the rule takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When Enable is unchecked, the rule does not take effect: the Pepwave router disregards the other parameters of the rule.</p> <p>Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.</p>														
Source	<p>This setting specifies the source IP Address, IP Network, MAC Address or Grouped Network for traffic that matches the rule.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Source</td> <td><input type="text" value="Any"/> ▾</td> </tr> <tr> <td>Destination</td> <td>Any</td> </tr> <tr> <td>Protocol</td> <td>IP Address</td> </tr> <tr> <td>Algorithm</td> <td>IP Network</td> </tr> <tr> <td></td> <td>MAC Address</td> </tr> <tr> <td></td> <td>Client Type</td> </tr> <tr> <td></td> <td>Client's Associated SSID</td> </tr> </table> </div>	Source	<input type="text" value="Any"/> ▾	Destination	Any	Protocol	IP Address	Algorithm	IP Network		MAC Address		Client Type		Client's Associated SSID
Source	<input type="text" value="Any"/> ▾														
Destination	Any														
Protocol	IP Address														
Algorithm	IP Network														
	MAC Address														
	Client Type														
	Client's Associated SSID														
Destination	This setting specifies the destination IP address, IP network, Domain name, SpeedFusion Cloud, SpeedFusion VPN Profile or Grouped network for traffic that matches the rule.														



If **Domain Name** is chosen and a domain name, such as *foobar.com*, is entered, any outgoing accesses to *foobar.com* and **.foobar.com* will match this criterion. You may enter a wildcard (*) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter *foobar.**, for example, *www.foobar.com*, *www.foobar.co.jp*, or *foobar.co.uk* will also match. Placing wildcards in any other position is not supported.

Note: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, access to any one of the server names will also match this rule.

Protocol and Port

This setting specifies the IP protocol and port of traffic that matches this rule. Via a drop-down menu, the following protocols can be specified:

- Any
- TCP
- UDP
- IP
- DSCP

Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.

Algorithm

This setting specifies the behavior of the Pepwave router for the custom rule.

One of the following values can be selected (Note that some Pepwave routers provide only some of these options):

- Weighted Balance
- Persistence
- Enforced
- Priority
- Overflow
- Least Used
- Lowest Latency
- Fastest Response Time

For a full explanation of each Algorithm, please see the following article:

<https://forum.peplink.com/t/exactly-how-do-peplinks-load-balancing-algorithms-work/8059>

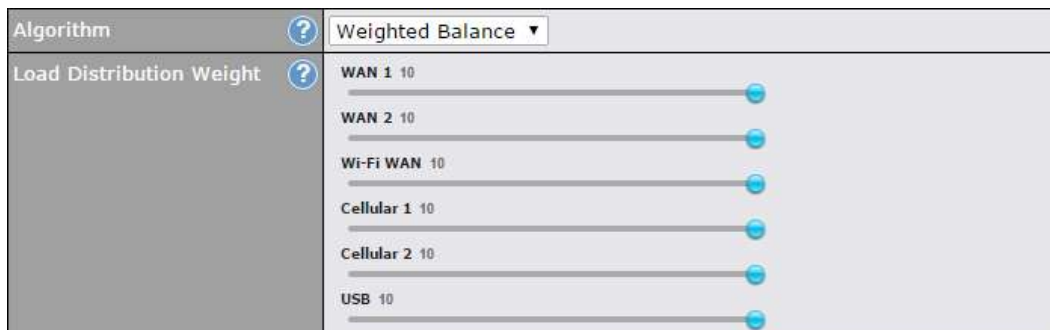
Load Distribution Weight

This is to define the outbound traffic weight ratio for each WAN connection.

<p>When No connections are available</p>	<p>This field allows you to configure the default action when all the selected Connections are not available.</p> <p>Drop the Traffic - Traffic will be discarded.</p> <p>Use Any Available Connections - Traffic will be routed to any available Connection, even it is not selected in the list.</p> <p>Fall-through to Next Rule - Traffic will continue to match the next Outbound Policy rule just like this rule is inactive.</p>
<p>Terminate Sessions on Connection Recovery</p>	<p>This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the Priority algorithms. By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.</p>

12.1.1 Algorithm: Weighted Balance

This setting specifies the ratio of WAN connection usage to be applied on the specified IP protocol and port. This setting is applicable only when **Algorithm** is set to **Weighted Balance**.



The amount of matching traffic that is distributed to a WAN connection is proportional to the weight of the WAN connection relative to the total weight. Use the sliders to change each WAN's weight.

For example, with the following weight settings:

- Ethernet WAN1: 10
- Ethernet WAN2: 10
- Wi-Fi WAN: 10
- Cellular 1: 10
- Cellular 2: 10

- USB: 10

Total weight is 60 = (10 +10 + 10 + 10 + 10 + 10).

Matching traffic distributed to Ethernet WAN1 is 16.7% = (10 / 60 x 100%).

Matching traffic distributed to Ethernet WAN2 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Wi-Fi WAN is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Cellular 1 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Cellular 2 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to USB is 16.7% = (10 / 60) x 100%.

12.1.2 Algorithm: Persistence

The configuration of persistent services is the solution to the few situations where link load distribution for Internet services is undesirable. For example, for security reasons, many e-banking and other secure websites terminate the session when the client computer's Internet IP address changes mid-session.

In general, different Internet IP addresses represent different computers. The security concern is that an IP address change during a session may be the result of an unauthorized intrusion attempt. Therefore, to prevent damages from the potential intrusion, the session is terminated upon the detection of an IP address change.

Pepwave routers can be configured to distribute data traffic across multiple WAN connections. Also, the Internet IP depends on the WAN connections over which communication actually takes place. As a result, a LAN client computer behind the Pepwave router may communicate using multiple Internet IP addresses. For example, a LAN client computer behind a Pepwave router with three WAN connections may communicate on the Internet using three different IP addresses.

With the persistence feature, rules can be configured to enable client computers to persistently utilize the same WAN connections for e-banking and other secure websites. As a result, a client computer will communicate using one IP address, eliminating the issues mentioned above.

Algorithm	Persistence
Persistence Mode	<input checked="" type="radio"/> By Source <input type="radio"/> By Destination
Load Distribution	<input type="radio"/> Auto <input checked="" type="radio"/> Custom
Load Distribution Weight	<ul style="list-style-type: none"> WAN 1 10 WAN 2 10 Wi-Fi WAN 10 Cellular 1 10 Cellular 2 10 USB 10

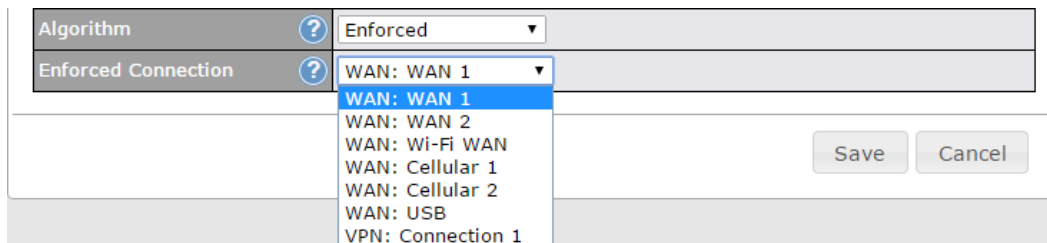
There are two persistent modes: **By Source** and **By Destination**.

By Source:	The same WAN connection will be used for traffic matching the rule and originating from the same machine, regardless of its destination. This option will provide the highest level of application compatibility.
By Destination:	The same WAN connection will be used for traffic matching the rule, originating from the same machine, and going to the same destination. This option can better distribute loads to WAN connections when there are only a few client machines.

The default mode is **By Source**. When there are multiple client requests, they can be distributed (persistently) to WAN connections with a weight. If you choose **Auto** in **Load Distribution**, the weights will be automatically adjusted according to each WAN's **Downstream Bandwidth** which is specified in the WAN settings page). If you choose **Custom**, you can customize the weight of each WAN manually by using the sliders.

12.1.3 Algorithm: Enforced

This setting specifies the WAN connection usage to be applied on the specified IP protocol and port. This setting is applicable only when **Algorithm** is set to **Enforced**.



Matching traffic will be routed through the specified WAN connection, regardless of the health check status of the WAN connection. Starting from Firmware 5.2, outbound traffic can be enforced to go through a specified SpeedFusion™ connection.

12.1.4 Algorithm: Priority

This setting specifies the priority of the WAN connections used to route the specified network service. The highest priority WAN connection available will always be used for routing the specified type of traffic. A lower priority WAN connection will be used only when all higher priority connections have become unavailable.

Algorithm	Priority	
Priority Order	Highest Priority	Not In Use
	WAN: WAN	
	WAN: Cellular 1	
	WAN: Cellular 2	
	WAN: USB	
	WAN: LAN 1 as WAN	
	WAN: GRE WAN 1	
	WAN: GRE WAN 2	
	WAN: OpenVPN WAN 1	
	Lowest Priority	
When No Connections are Available	Drop the Traffic	
Terminate Sessions on Connection Recovery	<input type="checkbox"/> Enable	

Starting from Firmware 5.2, outbound traffic can be prioritized to go through SpeedFusion™ connection(s). By default, VPN connections are not included in the priority list.

Tip

Configure multiple distribution rules to accommodate different kinds of services.

12.1.5 Algorithm: Overflow

The traffic matching this rule will be routed through the healthy WAN connection that has the highest priority and is not in full load. When this connection gets saturated, new sessions will be routed to the next healthy WAN connection that is not in full load.

Algorithm	Overflow	
Overflow Order	Highest Priority	
	WAN: WAN 1	
	WAN: WAN 2	
	WAN: Wi-Fi WAN	
	WAN: Cellular 1	
	WAN: Cellular 2	
	WAN: USB	
	Lowest Priority	

Drag and drop to specify the order of WAN connections to be used for routing traffic. Only the highest priority healthy connection that is not in full load will be used.

12.1.6 Algorithm: Least Used

Algorithm	Least Used
Connection	<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input checked="" type="checkbox"/> Wi-Fi WAN <input type="checkbox"/> Cellular 1 <input type="checkbox"/> Cellular 2 <input type="checkbox"/> USB

The traffic matching this rule will be routed through the healthy WAN connection that is selected in **Connection** and has the most available download bandwidth. The available download bandwidth of a WAN connection is calculated from the total download bandwidth specified on the WAN settings page and the current download usage. The available bandwidth and WAN selection is determined every time an IP session is made.

12.1.7 Algorithm: Lowest Latency

Algorithm	Lowest Latency <small>Note: Use of Lowest Latency will incur additional network usage.</small>
Connection	<input checked="" type="checkbox"/> WAN 1 <input checked="" type="checkbox"/> WAN 2 <input checked="" type="checkbox"/> Wi-Fi WAN <input type="checkbox"/> Cellular 1 <input type="checkbox"/> Cellular 2 <input type="checkbox"/> USB

The traffic matching this rule will be routed through the healthy WAN connection that is selected in **Connection** and has the lowest latency. Latency checking packets are issued periodically to a nearby router of each WAN connection to determine its latency value. The latency of a WAN is the packet round trip time of the WAN connection. Additional network usage may be incurred as a result.

Tip

The roundtrip time of a 6M down/640k uplink can be higher than that of a 2M down/2M up link because the overall round trip time is lengthened by its slower upload bandwidth, despite its higher downlink speed. Therefore, this algorithm is good for two scenarios:

- All WAN connections are symmetric; or
- A latency sensitive application must be routed through the lowest latency WAN, regardless of the WAN's available bandwidth.

12.1.8 Expert Mode

Expert Mode is available on some Pepwave routers for use by advanced users. To enable the feature, click on the help icon and click **turn on Expert Mode**.

In Expert Mode, a new special rule, **SpeedFusion™ Routes**, is displayed in the **Custom Rules** table. This rule represents all SpeedFusion™ routes learned from remote VPN peers. By default, this bar is on the top of all custom rules. This position means that traffic for remote VPN subnets will be routed to the corresponding VPN peer. You can create custom **Priority** or **Enforced** rules and move them

above the bar to override the SpeedFusion™ routes.

Upon disabling Expert Mode, all rules above the bar will be removed.

Help [Close](#)

This table allows you to fine tune how the outbound traffic should be distributed to the WAN connections.

Click the *Add Rule* button to add a new rule. Click the *X* button to remove a rule. Drag a rule to promote or demote its precedence. A higher position of a rule signifies a higher precedence. You may change the default outbound policy behavior by clicking the *Default* link.

If you require advanced control of PepVPN traffic, [turn on Expert Mode](#).

13 Port Forwarding

Pepwave routers can act as a firewall that blocks, by default, all inbound access from the Internet. By using port forwarding, Internet users can access servers behind the Pepwave router. Inbound port forwarding rules can be defined at **Advanced > Port Forwarding**.

Service	IP Address(es)	Server	Protocol
No Services Defined			
<input type="button" value="Add Service"/>			

To define a new service, click **Add Service**.

Port Forwarding
✕

Enable	<input checked="" type="checkbox"/>
Service Name	<input type="text"/>
Protocol	TCP ▾ ← :: Protocol Selection :: ▾
Port	Any Port ▾
Inbound IP Address(es) (Require at least one IP address) ?	<div style="display: flex; justify-content: space-between; align-items: center;"> Connection / IP Address(es) All Clear </div>
	<input type="checkbox"/> WAN
	<input type="checkbox"/> Cellular
	<input type="checkbox"/> Wi-Fi WAN on 2.4 GHz
	<input type="checkbox"/> Wi-Fi WAN on 5 GHz
<input type="checkbox"/> SpeedFusion VPN	
Server IP Address ?	<input type="text"/>


Port Forwarding Settings	
Enable	This setting specifies whether the inbound service takes effect. When Enable is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore “_” characters.

Protocol

The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Pepwave router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. Please see below for details on the **Port** and **Servers** settings. Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remain manually modifiable.

The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:

Any Port, Single Port, Port Range, Port Map, and Range Mapping

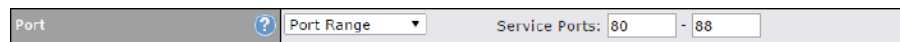


Any Port: all traffic that is received by the Pepwave router via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Any Port**, all TCP traffic is forwarded to the configured servers.



Single Port: traffic that is received by the Pepwave router via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Single Port** and **Service Port** 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80.

Port



Port Range: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Range** and **Service Ports** 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.



Port Mapping: traffic that is received by Pepwave router via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting.

For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Mapping**, **Service Port** 80, and **Map to Port** 88, TCP traffic on port 80 is forwarded to the configured servers via port 88.

(Please see below for details on the **Servers** setting.)

	<input type="text" value="Port"/>	<input type="text" value="Range Mapping"/>	Service Ports: <input type="text" value="80"/> - <input type="text" value="88"/> Map to Ports: <input type="text" value="88"/> - <input type="text" value="96"/>
<p>Range Mapping: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the Servers setting.</p>			
Inbound IP Address(es)	This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.		
Server IP Address	This setting specifies the LAN IP address of the server that handles the requests for the service.		

13.1 UPnP / NAT-PMP Settings

UPnP and NAT-PMP are network protocols which allow a computer connected to the LAN port to automatically configure the router to allow parties on the WAN port to connect to itself. That way, the process of inbound port forwarding becomes automated.

When a computer creates a rule using these protocols, the specified TCP/UDP port of all WAN connections' default IP address will be forwarded.

Check the corresponding box(es) to enable UPnP and/or NAT-PMP. Enable these features only if you trust the computers connected to the LAN ports.

UPnP / NAT-PMP Settings	
UPnP	<input type="checkbox"/> Enable
NAT-PMP	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

When the options are enabled, a table listing all the forwarded ports under these two protocols can be found at **Status > UPnP / NAT-PMP**.

14 NAT Mappings

NAT mappings allow IP address mapping of all inbound and outbound NAT'd traffic to and from an internal client IP address. Settings to configure NAT mappings are located at **Advanced > NAT Mappings**.

LAN Clients	Inbound Mappings	Outbound Mappings	
192.168.1.23	(WAN 1):10.88.3.158 (Interface IP)	Use <i>Interface IP</i> only	
Add NAT Rule			

To add a rule for NAT mappings, click **Add NAT Rule**.

NAT Mappings ✕

LAN Client	?	IP Address ▾									
IP Address		<input type="text"/>									
Inbound Mappings	?	Connection / Inbound IP Address(es) <ul style="list-style-type: none"> <input type="checkbox"/> WAN <input type="checkbox"/> Cellular <input type="checkbox"/> Wi-Fi WAN on 2.4 GHz <input type="checkbox"/> Wi-Fi WAN on 5 GHz <input type="checkbox"/> SpeedFusion VPN 									
Outbound Mappings	?	Connection / Outbound IP Address <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>WAN</td> <td>192.168.52.152 (Interface IP) ▾</td> </tr> <tr> <td>Cellular</td> <td>Interface IP ▾</td> </tr> <tr> <td>Wi-Fi WAN on 2.4 GHz</td> <td>Interface IP ▾</td> </tr> <tr> <td>Wi-Fi WAN on 5 GHz</td> <td>Interface IP ▾</td> </tr> </table>		WAN	192.168.52.152 (Interface IP) ▾	Cellular	Interface IP ▾	Wi-Fi WAN on 2.4 GHz	Interface IP ▾	Wi-Fi WAN on 5 GHz	Interface IP ▾
WAN	192.168.52.152 (Interface IP) ▾										
Cellular	Interface IP ▾										
Wi-Fi WAN on 2.4 GHz	Interface IP ▾										
Wi-Fi WAN on 5 GHz	Interface IP ▾										

[Save](#) [Cancel](#)

NAT Mapping Settings	
LAN Client	NAT mapping rules can be defined for a single LAN IP Address , an IP Range , or an IP Network .
IP Address	This refers to the LAN host's private IP address. The system maps this address to a number of public IP addresses (specified below) in order to facilitate inbound and outbound traffic. This option is only available when IP Address is selected.
IP Range	The IP range is a contiguous group of private IP addresses used by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when IP Range is selected.

IP Network	<p>The IP network refers to all private IP addresses and ranges managed by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when IP Network is selected.</p>
Inbound Mappings	<p>This setting specifies the WAN connections and corresponding WAN-specific Internet IP addresses on which the system should bind. Any access to the specified WAN connection(s) and IP address(es) will be forwarded to the LAN host. This option is only available when IP Address is selected in the LAN Client(s) field.</p> <p>Note that: inbound mapping is not needed for WAN connections in drop-in mode or IP forwarding mode. Also note that each WAN IP address can be associated to one NAT mapping only.</p>
Outbound Mappings	<p>This setting specifies the WAN IP addresses that should be used when an IP connection is made from a LAN host to the Internet. Each LAN host in an IP range or IP network will be evenly mapped to one of each selected WAN's IP addresses (for better IP address utilization) in a persistent manner (for better application compatibility).</p> <p>Note that: if you do not want to use a specific WAN for outgoing accesses, you should still choose default here, then customize the outbound access rule in the Outbound Policy section. Also note that WAN connections in drop-in mode or IP forwarding mode are not shown here.</p>

Click **Save** to save the settings when configuration has been completed.

Important Note

Inbound firewall rules override the **Inbound Mappings** settings.

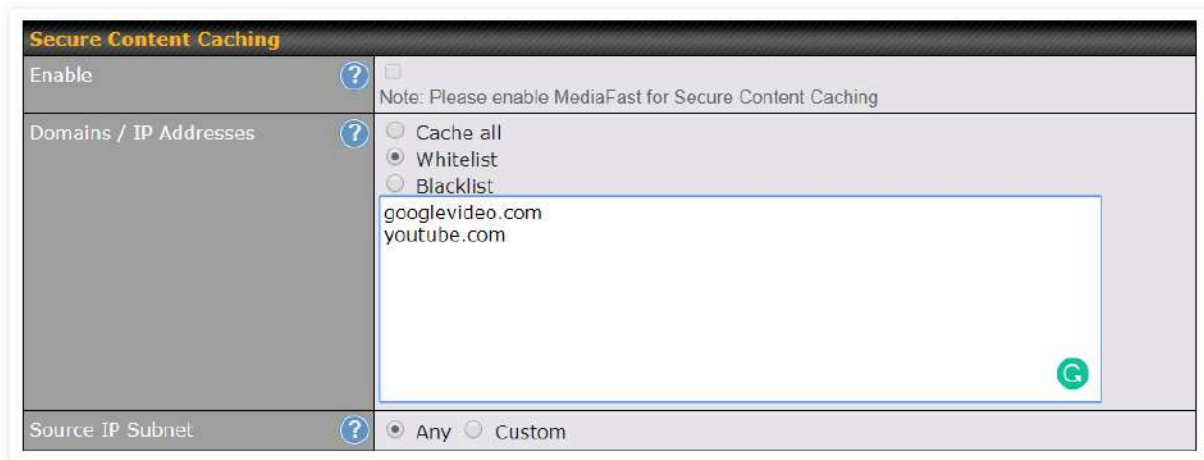
15 Media Fast

MediaFast settings can be configured from the **Advanced** menu.

15.1 Setting Up MediaFast Content Caching

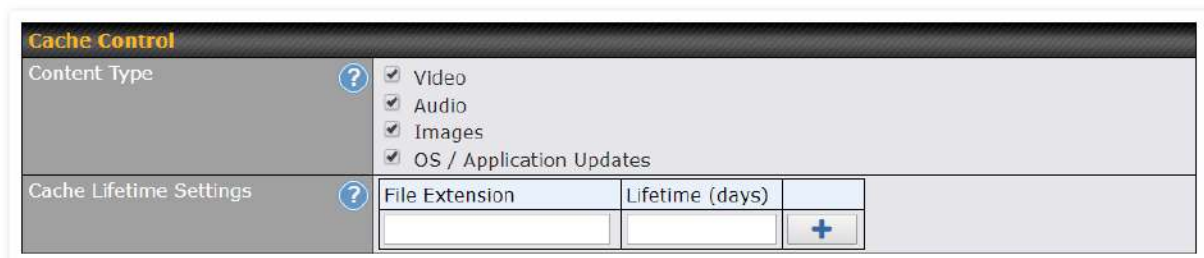
To access MediaFast content caching settings, select **Advanced > Cache Control**

MediaFast	
Enable	Click the checkbox to enable MediaFast content caching.
Domains / IP Addresses	Choose to Cache on all domains , or enter domain names and then choose either Whitelist (cache the specified domains only) or Blacklist (do not cache the specified domains).
Source IP Subnet	This setting allows caching to be enabled on custom subnets only. If "Any" is selected, then caching will apply to all subnets.



The **Secure Content Caching** menu operates identically to the **MediaFast** menu, except it is for secure content caching accessible through https://. In order for Mediafast devices to cache and deliver HTTPS content, every client needs to have the necessary certificates installed*.

*See <https://forum.peplink.com/t/certificate-installation-for-mediafast-https-caching/>



Cache Control	
Content Type	Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types.
Cache Lifetime Settings	Enter a file extension, such as JPG or DOC. Then enter a lifetime in days to specify how long files with that extension will be cached. Add or delete entries using the controls on the right.